УТВЕРЖДЕНЫ

Приказом Генерального директора

Акционерного общества «Марлин»

№5 от «27» февраля 2026 г.

ПРАВИЛА
Платежной системы МАРЛИН

(Редакция №1)

г. Кострома, 2026

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ....6

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ....7

3. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ МЕЖДУ ОПЕРАТОРОМ, УЧАСТНИКАМИ И ОПЕРАТОРАМИ УПИ 11

3.1. Структура Платежной системы МАРЛИН 11

3.2. Схема договорных отношений в Системе 12

4. ТРЕБОВАНИЯ К ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ ПЛАТЕЖНОЙ СИСТЕМЫ И ПРИВЛЕЧЕННЫХ ИМИ ЛИЦ....14

4.1. Права и обязанности Оператора 14

4.2. Права и обязанности Операционного центра 16

4.3. Права и обязанности Платежного клирингового центра 18

4.4. Права и обязанности Расчетного центра 20

4.5. Права и обязанности Участника.... 21

4.6. Особенности взаимодействия с Участниками-Иностранными поставщиками платежных услуг 24

4.7. Функции Банковского платежного агента 24

4.8. Партнеры Платежной системы МАРЛИН 25

5. УЧАСТИЕ В ПЛАТЕЖНОЙ СИСТЕМЕ 28

5.1. Виды и критерии участия в Платежной системе.... 28

5.2. Общие условия и порядок присоединения Участника к Системе.... 29

5.3. Критерии деятельности Участников в Системе.... 31

5.4. Критерии приостановления и прекращения участия в Системе.... 31

5.5. Порядок привлечения Операторов услуг платежной инфраструктуры.... 32

6. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ 35

6.1. Применяемые формы безналичных расчетов.... 35

6.2. Совершаемые операции 35

6.3. Порядок осуществления перевода денежных средств (приема, оформления и отправки новых Переводов), в т.ч. моменты наступления его безотзывности, безусловности и окончательности перевода 35

6.4. Порядок оформления, формирования и отправки запроса на изменение реквизитов ранее отправленного Перевода.... 40

6.5. Порядок оформления, формирования и отправки запросов на возврат Переводов 41

6.6. Порядок возврата Переводов, отвергнутых Получателем-юридическим лицом или кредитной организацией 44

6.7. Порядок получения, оформления и выдачи (зачисления) поступивших Переводов и Переводов к возврату 44

7. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖНОГО КЛИРИНГА И РАСЧЕТОВ....47

7.1. Порядок осуществления платежного клиринга 47

7.2. Порядок осуществления расчетов ... 48

7.3. Временно́й регламент осуществления платежного клиринга и расчетов ... 50

7.4. Порядок обеспечения исполнения обязательств Участников по переводу денежных средств 51

7.5. Порядок оплаты услуг по переводу денежных средств и услуг платежной инфраструктуры .. 52

7.6. Порядок оформления Актов оказанных услуг ... 58

8. СОБЛЮДЕНИЕ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА (ПОД/ФТ), И СОПРОВОЖДЕНИЮ ПЕРЕВОДА СВЕДЕНИЯМИ ОБ ОТПРАВИТЕЛЕ ... 59

8.1. Принципы и условия обработки персональных данных Клиентов в Системе ... 59

8.2. Принципы и условия осуществления деятельности в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Сопровождение перевода сведениями об Отправителе ... 61

9. СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ И ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОСТИ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ ... 63

9.1. Модель управления рисками ... 63

9.2. Мероприятия системы управления рисками ... 66

9.3. Организационная структура системы управления рисками Оператора ... 67

9.4. Способы управления рисками ... 68

9.5. Доведение до органов управления Оператора соответствующей информации о рисках ... 69

9.6. Показатели бесперебойности функционирования Платежной системы ... 69

9.7. Порядок обеспечения бесперебойности функционирования Платежной системы ... 73

9.8. Требования к методикам анализа рисков в Платежной системе, включая профили рисков ... 80

9.9. Порядок обмена информацией, необходимой для управления рисками ... 83

9.10. Порядок информационного взаимодействия Субъектов Платежной системы в спорных, чрезвычайных и нестандартных ситуациях, включая случаи системных сбоев ... 83

9.11. Контроль за соблюдением Субъектами Платежной системы порядка обеспечения БФПС 85

9.12. Порядок изменения операционных и технологических средств и процедур ... 85

9.13. Порядок оценки качества функционирования информационных систем, операционных и технологических средств ... 86

10. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНОЙ СИСТЕМЕ МАРЛИН ... 87

10.1. Общие требования к порядку обеспечения защиты информации ... 87

10.2. Порядок обеспечения защиты информации ... 91

10.3. Использование средств криптографической защиты информации ... 96

10.4. Оценка выполнения Участниками и Операторами УПИ требований к обеспечению защиты информации ... 97

10.5. Обеспечение совершенствования защиты информации ... 98

10.6. Мероприятия по противодействию осуществлению Переводов без добровольного согласия клиента 98

11. ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА ... 103

11.1. Термины и определения ... 103
11.2. Общие положения ... 105
11.3. Электронные сообщения и документы ... 105
11.4. Условия организации и правила осуществления ЭДО ... 106
11.5. Обеспечение информационной безопасности при ЭДО ... 108
11.6. Порядок разрешения конфликтных ситуаций, связанных с использованием ЭДО в Платежной системе МАРЛИН ... 110
11.7. Используемые ЭС и ЭП в Информационных системах Оператора ... 112
11.8. Требования к техническому и программному обеспечению осуществления операций 113
11.9. Права и обязанности Сторон при осуществлении ЭДО ... 114
11.10. Ответственность ... 115
12. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ ... 116
13. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ПРАВИЛ ... 118
13.1. Общие положения ... 118
13.2. Способы осуществления контроля ... 118
13.3. Действия Оператора при выявлении случаев нарушения Правил ... 118
14. ОТВЕТСТВЕННОСТЬ ЗА НЕСОБЛЮДЕНИЕ ПРАВИЛ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 120
15. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПРАВИЛА ... 122
16. ВЗАИМОДЕЙСТВИЕ С ИНЫМИ ПЛАТЕЖНЫМИ СИСТЕМАМИ ... 124
ПРИЛОЖЕНИЕ №1 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 125
ПРИЛОЖЕНИЕ №2 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 126
Приложение №2.1. Проект формы Договора участия в Платежной системе для Прямого участника 126
Приложение №2.2. Проект формы Договора участия в Платежной системе для Косвенного участника 130
ПРИЛОЖЕНИЕ №3 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 135
ТАРИФЫ ... 135
ПРИЛОЖЕНИЕ №4 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 137
ПРИЛОЖЕНИЕ №5 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 147
ПРИЛОЖЕНИЕ №6 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 149
ПРИЛОЖЕНИЕ №7 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 151
ПРИЛОЖЕНИЕ №8 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ... 153
1. Классификация рисков в Платежной системе МАРЛИН ... 153
2. Анализ бизнес-процессов в Платежной системе МАРЛИН ... 155
3. Порядок выявления и анализа рисков Платежной системы, включая выявление риск-событий, и порядок определения для каждого из выявленных риск-событий уровня риска ... 156
4. Порядок определения для каждого из выявленных рисков в Платежной системе уровня присущего риска, а также уровня допустимого риска ... 160
5. Порядок определения рисков, значимых для Платежной системы ... 160

6. Порядок определения уровня остаточного риска. Мониторинг рисков 160

7. Перечень риск-событий, причин риск-событий и способов управления рисками Платежной системы. 161

ПРИЛОЖЕНИЕ №9 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН 163

ПРИЛОЖЕНИЕ №10 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН 170

ПРИЛОЖЕНИЕ №11 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН 171

ПРИЛОЖЕНИЕ №12 К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН 184

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Платежная система МАРЛИН (далее также «Платежная система», «Система», «ПС») 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 МАРЛИН в целях осуществления переводов денежных средств, в том числе услуг по трансграничному переводу денежных средств.

1.2. Оператором Платежной системы МАРЛИН является Акционерное общество «Марлин» (ОГРН 1254400003428, ИНН 4400026113, адрес местонахождения: 156013, Костромская область, г.о. Кострома, г. Кострома, ул. Горького, д. 8Б).

1.3. Настоящие Правила Платежной системы МАРЛИН (далее – «Правила») составлены в виде единого документа и определяют порядок, условия и особенности взаимодействия Оператора Системы, Операторов услуг платежной инфраструктуры и Участников Системы при осуществлении переводов денежных средств, в том числе с использованием различных Электронных средств платежа в рамках применяемых форм безналичных расчетов.

1.4. Правила Платежной системы разрабатывает и вводит в действие Оператор Системы. Настоящие правила разработаны в соответствии с требованиями Федерального закона от 27 июня 2011 года «О национальной платежной системе» №161-ФЗ (далее – «Федеральный закон №161-ФЗ») и принятыми в соответствии с ним нормативными актами Банка России. Отношения Субъектов Платежной системы регулируются в соответствии с законодательством Российской Федерации.

1.5. Настоящие Правила Платежной системы МАРЛИН являются договором присоединения, который заключается в соответствии со статьей 428 Гражданского кодекса Российской Федерации. В случае обнаружения каких-либо противоречий, несоответствий, содержащихся в условиях Правил и договора, заключенного Оператором Системы с Субъектами Платежной системы, приоритетными являются положения Правил Системы.

1.6. Правила, включая Тарифы Системы, являются публично доступными и размещаются на официальном сайте Оператора в информационно-телекоммуникационной сети Интернет по адресу: www.marlinpay.ru.

1.7. Настоящие Правила обязательны для исполнения всеми Субъектами Платежной системы.

1.8. Настоящие Правила Платежной системы МАРЛИН вступают в силу с даты государственной регистрации Оператора в реестре операторов платежных систем Банка России.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Банковский платежный агент (БПА) – юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые на основании договора привлекаются Участником в целях осуществления отдельных банковских операций.

Банковский платежный субагент (БПСА) – юридическое лицо, не являющееся кредитной организацией, или индивидуальный предприниматель, которые на основании договора привлекаются БПА для выполнения своих функций, предусмотренных договором с Участником в целях осуществления отдельных банковских операций.

Безадресный перевод – перевод денежных средств, при котором Отправитель не указывает конкретный пункт Участника Системы, в котором будут получены денежные средства.

Безотзывность перевода денежных средств – характеристика перевода денежных средств, обозначающая отсутствие или прекращение возможности отзыва Распоряжения об осуществлении перевода денежных средств в определенный момент времени.

Безусловность перевода денежных средств – характеристика перевода денежных средств, обозначающая отсутствие условий или выполнение всех условий для осуществления перевода денежных средств в определенный момент времени.

Бивалютный перевод – перевод денежных средств, при котором валюта отправки перевода, осуществленного Отправителем, отличается от валюты выдачи перевода Получателю.

ДБО – дистанционное банковское обслуживание.

Иностранный поставщик платежных услуг – иностранная организация, имеющая право в соответствии с законодательством иностранного государства, на территории которого она зарегистрирована, на основании лицензии или иного разрешения оказывать услуги по переводу денежных средств по банковским счетам и(или) без открытия банковских счетов и(или) осуществлять операции с использованием Электронных средств платежа[1].

Информационно-справочный центр – информационно-консультационный центр Оператора, предназначенный для сбора информации, консультирования и оказания помощи Клиентам.

Клиент – Отправитель и(или) Получатель.

Лимит Участника (ЛУ) – предельный размер обязательств Участника в соответствующей валюте, в пределах которой в Системе могут быть выполнены операции по переводу денежных средств в пользу другого Участника или другой платежной системы, с которой Оператор установил межсистемное взаимодействие в порядке, предусмотренном настоящими Правилами. Лимит Участника формируется, как правило, за счет денежных средств, перечисленных Участником Расчетному центру/Прямому участнику. ЛУ постоянно меняется в соответствии с суммами операций. Каждая операция оплаты автоматически уменьшает или увеличивает ЛУ соответствующего Участника.

Личный кабинет Участника (далее – ЛК) - информационная система Оператора, представляющая собой клиент-серверное приложение, доступное из браузера по URL, обеспечивающее доступ к ПО Системы и предназначенное для сотрудников Участника (Партнеров, БПА, БПСА), позволяющее получать справочную информацию, управлять частью инфраструктуры Участника (Партнеров, БПА, БПСА) в рамках Системы, а также осуществлять информационный обмен с Оператором.

Окончательность перевода денежных средств – характеристика перевода денежных средств, обозначающая предоставление денежных средств Получателю в определенный момент времени.

Оператор Платежной системы (Оператор, Оператор Системы) – Акционерное общество «Марлин» (ОГРН 1254400003428), определяющее Правила Платежной системы МАРЛИН, а также

[1] Уведомление Банку России направляется Оператором Системы в случае заключения договора с ИППУ в целях обеспечения возможности приема на территории Российской Федерации электронных средств платежа в соответствии со ст. 9.1 Федерального закона №161-ФЗ.

выполняющее иные обязанности, предусмотренные Федеральным законом «О национальной платежной системе» и Правилами Платежной системы МАРЛИН.

Оператор услуг платежной инфраструктуры (Оператор УПИ) – юридические лица и кредитные организации, исполняющие в соответствии с законодательством Российской Федерации, Правилами и договором с Оператором (при наличии) функции Операционного центра, Платежного клирингового центра и Расчетного центра.

Оператор по переводу денежных средств – кредитная организация, в соответствии с законодательством Российской Федерации имеющая право осуществлять перевод денежных средств.

Оператор электронных денежных средств – Оператор по переводу денежных средств, осуществляющий перевод Электронных денежных средств без открытия банковского счета (перевод Электронных денежных средств).

Операционный центр (ОЦ) – организация, обеспечивающая для Участников и их Клиентов доступ к услугам по переводу денежных средств, в том числе с использованием ЭСП, а также осуществляющая информационное и технологическое взаимодействие между Субъектами Системы.

Отчет(ы) Участника (Отчет(ы)) – электронный(е) документ(ы), формируемый(е) Платежным клиринговым центром в разрезе валют по итогам закрытого отчетного периода, направляемый(е) Участнику в целях проведения взаиморасчетов по совершенным в Системе операциям, или подтверждающий(е) проведение Расчетным центром взаиморасчетов по Распоряжениям за закрытый отчетный период.

Отчет по операциям ЦПКК – электронный документ, формируемый Платежным клиринговым центром по результатам совершенных операций в течение операционного дня, содержащий сведения о переводах денежных средств, подлежащих зачислению и(или) списанию по Счетам ЦПКК.

Отправитель – физическое или юридическое лицо, индивидуальный предприниматель, осуществляющее в рамках Системы операции по переводу денежных средств в пользу Получателя. В случае если законодательством страны инкорпорации Участника предусмотрены ограничения на осуществление переводов денежных средств отдельными лицами, являющимися Отправителями в соответствии с настоящими Правилами, Отправителем может являться только то лицо, обслуживание которого в рамках Платежной системы допустимо с точки зрения законодательства страны инкорпорации Участника.

Партнер – российская или иностранная кредитная или иная организация, обладающая необходимым разрешением (лицензией) на право осуществления переводов денежных средств по поручениям физических лиц в соответствии с законодательством государства, на территории которого она зарегистрирована, осуществляющая перевод в соответствии с соглашениями, заключенными с Участниками, требования к которым устанавливаются настоящими Правилами.

Перевод денежных средств (Перевод) – действия Участника в рамках применяемых форм безналичных расчетов и настоящих Правил по предоставлению Получателю денежных средств Отправителя.

Платежный клиринговый центр (ПКЦ) – организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках Платежной системы МАРЛИН прием к исполнению Распоряжений Участников Платежной системы об осуществлении перевода денежных средств и выполнение иных действий, предусмотренных Федеральным законом №161-ФЗ и Правилами Платежной системы.

Получатель – физическое или юридическое лицо, индивидуальный предприниматель, в пользу которого осуществляется перевод денежных средств от Отправителя. В случае если законодательством страны инкорпорации Участника предусмотрены ограничения на осуществление переводов денежных средств в пользу отдельных лиц, являющихся Получателями в соответствии с настоящими Правилами, Получателем может являться только то лицо, обслуживание которого в рамках Платежной системы допустимо с точки зрения законодательства страны инкорпорации Участника.

Программное обеспечение Системы (ПО Системы) – комплекс программного обеспечения (программных средств) Системы, предоставляющий Субъектам и привлеченным ими лицам доступ к Системе, взаимодействующего(-их) между собой с применением информационных и коммуникационных технологий, обеспечивающих прием, передачу, хранение и обработку информации о переводах денежных средств, точках обслуживания клиентов, о расчетах между Сторонами, проводимых в связи с осуществлением переводов денежных средств, а также к получению иной информации, необходимой Субъектам и привлеченным ими лицам для исполнения заключенных ими договоров.

Распоряжение – расчетный документ, сформированный Участником и содержащий информацию, позволяющую осуществить перевод денежных средств в рамках Платежной системы.

Расчетный центр (РЦ) – организация, созданная в соответствии с законодательством Российской Федерации, обеспечивающая в рамках Платежной системы МАРЛИН исполнение Распоряжений Участников Платежной системы МАРЛИН посредством списания и зачисления денежных средств по Счетам Участников Платежной системы МАРЛИН, а также направление подтверждений, касающихся исполнения Распоряжений Участников Платежной системы МАРЛИН (далее – расчетные услуги).

Реестр расчетных документов (Реестр) – электронный документ, формируемый Платежным клиринговым центром по результатам платежного клиринга, включающий в себя итоговые суммы платежно-клиринговых позиций Субъектов, который подлежит направлению в Расчетный центр для осуществления расчетов между Субъектами Системы посредством списания и/или зачисления денежных средств по Счетам Участников и(или) по Счетам ЦПКК.

Согласованные каналы связи – средства и способы, определенные Оператором Системы и соответствующим Субъектом для обмена информацией, не носящей платежный характер и не содержащей банковскую тайну. Каналы связи для обмена информацией, содержащей платежные данные, определяются предоставленными Стороне доступами в Систему в рамках порядка электронного документооборота, предусмотренного настоящими Правилами.

Субъекты Платежной системы (Субъекты Системы) – лица, указанные в п. 3.1.1. Правил.

Счет Участника (Счет) – счет Участника, предназначенный для осуществления расчетов в Платежной системе, открываемый: для Прямых участников – в Расчетном центре Системы, для Косвенных участников – у Прямых участников Системы.

Счет Центрального платежного клирингового контрагента (Счет ЦПКК) – счет ЦПКК, который открывается для учета переводов денежных средств в соответствующей валюте, по которым ЦПКК выступает Отправителем и получателем денежных средств по переводам денежных средств Участников Платежной Системы.

Тарифы Системы (Тарифы) – документ Оператора, устанавливающий размер и условия взимания платы за оказание услуг по переводу денежных средств в рамках Платежной системы.

Услуги Системы – оказываемые Участниками и(или) привлеченными ими лицами услуги по осуществлению перевода 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 карты и(или) счета физических лиц в кредитных организациях;

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

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

е) от юридических лиц/индивидуальных предпринимателей для выплаты физическим лицам, при предоставлении полных реквизитов платежа.

Перечень типов переводов денежных средств, доступных Участнику и(или) Партнеру при получении Услуг Системы, может быть ограничен в случае, если законодательством страны инкорпорации Участника и(или) Партнера предусмотрено ограничение и(или) запрет на их осуществление с использованием Системы.

Участники Платежной системы (Участники) – организации, присоединившиеся к Правилам Платежной системы МАРЛИН в целях оказания услуг по переводу денежных средств. По видам участия в Платежной системе МАРЛИН Участники подразделяются на Прямых и Косвенных. Если иное прямо не указано в настоящих Правилах, права и обязанности Участников, предусмотренные Правилами, а также требования Оператора к порядку осуществления ими деятельности в Платежной системе МАРЛИН, распространяются как на Прямых, так и на Косвенных участников.

Участник-отправитель – Участник, осуществляющий прием наличных денежных средств, или списание денежных средств со счета Отправителя для осуществления перевода денежных средств.

Участник-получатель – Участник, осуществляющий выдачу денежных средств в наличной форме или зачисление денежных средств на счет Получателю.

Центральный платежный клиринговый контрагент (ЦПКК) – платежный клиринговый центр, выступающий в соответствии с Федеральным законом №161-ФЗ плательщиком и получателем средств по переводам денежных средств Участников Платежной системы.

Электронная подпись (ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связанная с такой информацией и которая используется для определения лица, подписывающего информацию.

Электронные денежные средства (ЭДС) – 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. При этом не являются Электронными денежными средствами денежные средства, полученные организациями, осуществляющими профессиональную деятельность на рынке ценных бумаг, клиринговую деятельность, деятельность оператора финансовой платформы, деятельность по организации привлечения инвестиций, деятельность по управлению инвестиционными фондами, паевыми инвестиционными фондами и негосударственными пенсионными фондами, деятельность операторов информационных систем, в которых осуществляется выпуск цифровых финансовых активов, и (или) деятельность операторов обмена цифровых финансовых активов и осуществляющими учет информации о размере предоставленных денежных средств без открытия банковского счета в соответствии с законодательством, регулирующим деятельность указанных организаций.

Электронный документооборот (ЭДО) – обмен электронными документами в соответствии с условиями, определенными Оператором в соответствии с настоящими Правилами и иными документами Оператора Системы.

Электронное средство платежа (ЭСП) – средство и (или) способ, позволяющие Клиенту 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.

3. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ МЕЖДУ ОПЕРАТОРОМ, УЧАСТНИКАМИ И ОПЕРАТОРАМИ УПИ

3.1. Структура Платежной системы МАРЛИН

3.1.1. Субъектами Платежной системы являются:

- Оператор Системы;
- Операторы УПИ:
  - Операционный центр;
  - Платежный клиринговый центр;
  - Расчетный центр;
  - ЦПКК (при необходимости).
- Участники Системы.

3.1.2. Субъекты осуществляют свою деятельность в рамках Системы на основании настоящих Правил и соответствующих договоров, заключенными между Субъектами.

3.1.3. Оператор определяет Правила Системы и осуществляет контроль за их соблюдением Субъектами Системы. Оператор выполняет организационные функции и координирует деятельность Субъектов Системы в соответствии с их статусами в Системе на основании настоящих Правил и договоров.

3.1.4. Оператор обеспечивает взаимодействие между Субъектами в соответствии с настоящими Правилами и заключенными между Субъектами Системы договорами.

3.1.5. Оператор в рамках Системы совмещает свою деятельность с деятельностью Оператора УПИ: Операционного центра и Платежного клирингового центра.

3.1.6. Оператор в рамках Системы может совмещать свою деятельность с деятельностью БПА и(или) БПСА.

3.1.7. Оператор осуществляет привлечение Операторов УПИ: Расчетные центры, дополнительные Операционные центры и Платежные клиринговые центры, в том числе выполняющие функции ЦПКК (при необходимости).

3.1.8. В Платежной системе возможно участие нескольких Расчетных центров, Операционных центров и Платежных клиринговых центров, в том числе выполняющих функции ЦПКК.

3.1.9. Оператор УПИ, не являющийся кредитной организацией, может совмещать оказание операционных услуг, услуг платежного клиринга. Оператор УПИ, являющийся кредитной организацией, может совмещать оказание операционных услуг, услуг платежного клиринга, услуг центрального платежного клирингового контрагента и расчетного центра.

3.1.10. Участники присоединяются к Правилам и осуществляют свою деятельность в рамках Системы на основании Договора участия с Оператором.

3.1.11. Участники Системы могут совмещать свою деятельность с деятельностью Операторов УПИ для оказания в Платежной системе операционных услуг, услуг платежного клиринга, расчетных услуг, услуг центрального платежного клирингового контрагента при условии соответствия Участника требованиям законодательства Российской Федерации для выполнения функций соответствующего Оператора УПИ.

3.1.12. Для реализации своих прав и обязанностей в рамках Системы Участники могут на основании договора привлекать Партнеров, а также БПА, которые, в свою очередь, на основании договора имеют право привлекать БПСА.

3.1.13. Взаимодействие между Оператором и Участниками, Оператором и привлеченными Операторами УПИ, Участниками и привлеченными Операторами УПИ осуществляется в рамках их прав и обязанностей, установленных действующим законодательством Российской Федерации, настоящими Правилами и договорами, заключенными с Оператором и между Субъектами (в случае их наличия).

3.1.14. Субъекты Системы обязаны:

- гарантировать банковскую тайну в соответствии с применимым законодательством;
- обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России;
- 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.

3.1.15. Оператор Системы, Операторы УПИ, Участники, а также привлекаемые ими лица (далее – «Стороны») при исполнении своих обязательств в рамках Правил, их аффилированные лица, работники и (или) посредники:

- не выплачивают, не предлагают выплатить, не разрешают выплату каких-либо денежных средств или ценностей, прямо или косвенно, любым лицам, для оказания влияния на действия или решения этих лиц с целью получить какие-либо неправомерные преимущества или иные неправомерные цели;
- не осуществляют действия, квалифицируемые применимым для целей Правил законодательством, как дача/получение взятки, коммерческий подкуп, а также действия, нарушающие требования применимого законодательства и международных актов о противодействии легализации (отмыванию) доходов, полученных преступным путем.

В случае возникновения у какой-либо из Сторон подозрений, что произошло или может произойти нарушение каких-либо положений предыдущих абзацев настоящего пункта, соответствующая Сторона обязуется уведомить Оператора Системы в письменной форме.

В письменном уведомлении Сторона обязана сослаться на факты или предоставить материалы, достоверно подтверждающие или дающие основание предполагать, что произошло или может произойти нарушение каких-либо положений настоящего пункта кем-либо из Сторон, его аффилированными лицами, работниками или посредниками выражающееся в действиях, квалифицируемых применимым законодательством, как дача или получение взятки, коммерческий подкуп, а также действиях, нарушающих требования применимого законодательства и международных актов о противодействии легализации доходов, полученных преступным путем.

После письменного уведомления соответствующая Сторона имеет право приостановить исполнение обязательств в рамках Правил до получения подтверждения, что нарушения не произошло или не произойдет. Это подтверждение должно быть направлено в течение 10 (десяти) рабочих дней с момента направления письменного уведомления.

3.2. Схема договорных отношений в Системе

3.2.1. Системообразующие договоры:

3.2.1.1. Договор Оператора с Операционным центром и Платежным клиринговым центром (в случае их привлечения Оператором). Договоры с Операционным центром и с Платежным клиринговым центром могут быть объединены в одном договоре, если эти функции выполняет один Субъект;

3.2.1.2. Договор Оператора с Расчетным центром;

3.2.1.3. Договор Оператора с Платежным клиринговым центром, выполняющим функции ЦПКК (в случае его привлечения Оператором). Договоры Оператора с Расчетным центром и с ПКЦ, выступающим в качестве ЦПКК, могут быть объединены в одном договоре, если эти функции выполняет один Субъект;

3.2.2. Для присоединения к Правилам и оказания услуг, поддерживаемых Платежной системой, Участник заключает следующие договоры:

3.2.2.1. Договор участия в Системе с Оператором (проекты форм Договоров участия содержатся в Приложении №2 и могут быть изменены по соглашению между Оператором и Участником);

3.2.2.2. Договор об открытии банковского счета Участника в Расчетном центре/у Прямого участника (по форме Расчетного центра/Прямого участника). Договор об открытии банковского счета подлежит заключению теми Косвенными участниками, которые осуществляют деятельность операторов по переводу денежных средств (включая Операторов электронных денежных средств). Договор банковского счета с Прямым участником могут не заключать Косвенные участники, являющиеся международной финансовой организацией, иностранным центральным (национальным) банком, иностранным банком (иностранной кредитной организацией), Иностранным поставщиком платежных услуг (далее – «Иные Косвенные участники»), при этом отношения Прямого и Иного Косвенного участника в части взаиморасчетов по операциям, совершенным в Системе, регулируются отдельным договором, условия которого не должны противоречить настоящим Правилам;

3.2.2.3. Договор оказания операционных услуг с Операционным центром (в случае привлечения Оператором Операционного центра);

3.2.2.4. Договор об оказании платежных клиринговых услуг с Платежным клиринговым центром (в случае привлечения Оператором Платежного клирингового центра).

Договоры с Операционным центром и с Платежным клиринговым центром могут быть объединены в одном договоре, если эти функции выполняет один Субъект.

3.2.3. Договоры Участников (по форме Участника):

3.2.3.1. Договор Участника с Партнером;

3.2.3.2. Договор Участника с БПА.

3.2.4. Договорные отношения Участника/Оператора и Клиента регулируются договором, который может заключаться в виде оферты Оператора/Участника, содержащей условия осуществления переводов денежных средств в рамках Платежной системы, который не должен противоречить настоящим Правилам, а также должен соответствовать существенным условиям, определенным Оператором в настоящих Правилах, обусловленным технологическими особенностями функционирования Системы и общими требованиями к качеству обслуживания Клиентов.

3.2.5. Договорные отношения между Прямым участником и Косвенным участником, Участником и Партнером, Участником и БПА не должны противоречить настоящим Правилам и должны содержать права и обязанности в соответствии с требованиями настоящих Правил.

4. ТРЕБОВАНИЯ К ДЕЯТЕЛЬНОСТИ СУБЪЕКТОВ ПЛАТЕЖНОЙ СИСТЕМЫ И ПРИВЛЕЧЕННЫХ ИМИ ЛИЦ

4.1. Права и обязанности Оператора

4.1.1. Оператор обязан:

4.1.1.1. Определять Правила Системы и осуществлять контроль за их соблюдением Участниками и Операторами УПИ.

4.1.1.2. Разрабатывать Правила Системы в соответствии с требованиями законодательства Российской Федерации.

4.1.1.3. Контролировать и обеспечивать соответствие настоящих Правил действующему законодательству Российской Федерации. Учитывать все изменения законодательства Российской Федерации, нормативных актов Правительства и Банка России путем внесения соответствующих изменений в Правила.

4.1.1.4. Осуществлять привлечение Операторов УПИ, которые соответствуют требованиям Федерального закона №161-ФЗ.

4.1.1.5. Привлекать в качестве Расчетных центров кредитные организации, которые не менее 1 (одного) года осуществляют перевод денежных средств по открытым в этой кредитной организации банковским счетам.

4.1.1.6. Вести перечень Операторов УПИ.

4.1.1.7. Обеспечивать бесперебойность оказания услуг платежной инфраструктуры Участникам.

4.1.1.8. Обеспечивать восстановление надлежащего функционирования Платежной системы в случае его нарушения, в том числе восстановление оказания услуг платежной инфраструктуры;

4.1.1.9. Информировать Банк России и Участников о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в порядке, установленном настоящими Правилами.

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

4.1.1.11. Организовывать систему управления рисками в Платежной системе в соответствии с действующим законодательством Российской Федерации, осуществлять оценку и управление рисками в Платежной системе, обеспечивать бесперебойность функционирования Платежной системы (далее – «БФПС») в порядке, установленном Банком России.

4.1.1.12. Обеспечивать возможность досудебного и (или) третейского рассмотрения споров с Участниками и Операторами УПИ в соответствии с настоящими Правилами.

4.1.1.13. Определять порядок защиты информации при осуществлении переводов денежных средств в Платежной системе с учетом требований, содержащихся в действующем законодательстве и нормативных актах Банка России.

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

4.1.1.15. Своевременно информировать Участников об изменениях в настоящих Правилах в соответствии с порядком, установленным настоящими Правилами.

4.1.1.16. Представлять в Банк России изменения Правил Платежной системы, изменения перечня Операторов УПИ не позднее 10 дней со дня внесения соответствующих изменений.

4.1.1.17. В соответствии с порядком, определенным настоящими Правилами, осуществлять функции Операционного центра и Платежного клирингового центра, обеспечивать Участникам доступ к информации, необходимой для работы в Системе.

4.1.1.18. Предоставлять организациям, намеревающимся участвовать в Платежной системе, Правила для предварительного ознакомления без взимания платы, за исключением расходов на изготовление копий Правил.

4.1.1.19. Выявлять в Системе организации, предоставляющие 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, осуществлять привлечение указанных организаций в качестве Операторов УПИ.

4.1.1.20. Поддерживать информацию, касающуюся функционирования Системы, в актуальном состоянии и обеспечивать возможность доступа к ней со стороны Участников.

4.1.1.21. В случае приостановления работы Системы в рамках плановых профилактических работ за 3 (три) дня уведомить Участников о времени и длительности планируемых к проведению работ. В случае проведения внеплановых технических работ Оператор уведомляет Субъектов Платежной системы не позднее чем за 15 (пятнадцать) минут до их начала.

4.1.1.22. Обеспечить круглосуточный прием обращений Клиентов и Участников Системы.

4.1.1.23. Указывать свой регистрационный номер при предоставлении информации о Платежной системе (присвоенный при регистрации и внесенный в реестр операторов платежных систем в соответствии со статьей 15 Федерального закона №161-ФЗ) любым другим лицам.

4.1.1.24. Реализовывать мероприятия, направленные на противодействие осуществлению переводов денежных средств без добровольного согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием (далее при совместном упоминании – «перевод денежных средств без добровольного согласия клиента»).

4.1.2. Оператор имеет право:

4.1.2.1. В одностороннем порядке вносить изменения в настоящие Правила в соответствии с требованиями законодательства РФ и порядком, предусмотренным настоящими Правилами.

4.1.2.2. Вносить изменения в Тарифы в соответствии с настоящими Правилами в одностороннем порядке.

4.1.2.3. Ограничивать возможность совершения Участником и(или) Партнером отдельных типов Переводов, по которым им предоставляются Услуги Системы, в случае, если законодательством страны инкорпорации Участника предусмотрено ограничение и(или) запрет на их осуществление с использованием Системы.

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

4.1.2.5. Определять Расчетный центр для Участника Платежной системы, а также порядок взаимодействия с ним.

4.1.2.6. Принимать решение о начале или прекращении участия в Платежной системе отдельных Участников в порядке и по основаниям, установленным настоящими Правилами.

4.1.2.7. Приостанавливать (блокировать) обслуживание Участника в целях предотвращения (прекращения) действий, нарушающих условия настоящих Правил. Основаниями для приостановления (блокирования) обслуживания Участника являются:

– несвоевременное формирование минимальной (неснижаемой) величины Лимита Участника (если это установлено Договором) путем перечисления денежных средств на Счет, открытый в Расчетном центре;

– несвоевременное и/или неполное перечисление в Расчетный центр суммы денежных средств, принятой от Клиентов за операционный день, совершенное неоднократно в течение календарного месяца;

– неоднократное нарушение Участником срока уплаты вознаграждения Оператору или другому Субъекту Системы, когда задержка уплаты составила более 10 (Десяти) календарных дней;

– выявления иных ненадлежащих и/или неправомерных действий Участника, наносящих вред (ущерб) иным Участникам, Оператору или Системе в целом.

4.1.2.8. Заключать договоры о взаимодействии с другими платежными системами согласно порядку такого взаимодействия, изложенного в настоящих Правилах.

4.1.2.9. Совершенствовать технологические процессы работы Системы, своевременно извещая об изменениях Участников.

4.1.2.10. Запрашивать и получать информацию от Субъектов Системы, в том числе внутренние документы и договоры, в связи с осуществлением ими деятельности в рамках Платежной системы.

4.1.2.11. Устанавливать и изменять требования по защите информации при осуществлении перевода денежных средств.

4.1.2.12. Ссылаться на работу Участника в Системе в рекламных и информационных целях. Упоминать Участника в своих рекламных и информационных материалах в маркетинговых целях и в целях развития Системы.

4.1.2.13. Взимать вознаграждение с Участников (выплачивать Участникам) в соответствии с Тарифами Системы и условиями заключенных договоров за услуги, оказываемые Оператором Участникам.

4.1.2.14. Рассматривать жалобы Клиентов Участников (их Партнеров, БПА/БПСА) на действия (бездействие) Участников при оказании услуг Участниками (их Партнеров, БПА/БПСА); применять к Участникам санкции, предусмотренные настоящими Правилами.

4.1.2.15. Привлекать третьих лиц для оказания информационно-технологических, а также иных видов услуг, прямо или косвенно связанных с выполнением Оператором Системы функций, возложенных на него настоящими Правилами, без дополнительного согласования с Участниками Системы.

4.1.2.16. Устанавливать требования к договорам, заключаемым между Участником и Партнером, Прямым и Иным Косвенным участником, Участником и БПА в целях осуществления расчетов по операциям в Системе.

4.2. Права и обязанности Операционного центра

4.2.1. **Операционный центр обязан**:

4.2.1.1. Осуществлять свою деятельность в соответствии с настоящими Правилами и на основании договоров об оказании операционных услуг с Оператором (в случае привлечения Оператором Операционного центра), с Операторами УПИ, указанными Оператором, и Участниками (в случае привлечения Оператором Операционного центра).

4.2.1.2. Обеспечивать обмен электронными сообщениями между: Участниками, между Участниками и Клиентами, Платежным клиринговым центром, Расчетным центром, между Платежным клиринговым центром и Расчетным центром. Операционный центр может осуществлять иные действия, связанные с использованием информационно-коммуникационных технологий, необходимые для функционирования Платежной системы.

4.2.1.3. Обеспечивать доступ Участников к техническим ресурсам Системы в целях оказания Услуг Системы.

4.2.1.4. Выполнять следующие функции:

- определять необходимый перечень программного обеспечения и использовать его для обеспечения функционирования Системы, определять порядок его использования Участниками;
- определять требования к оборудованию и технологическим решениям, используемым Участниками;
- обеспечивать регистрацию (интеграцию) Участников в Системе;
- обеспечивать для Участников и их Клиентов доступ к услугам по переводу денежных средств, в том числе с использованием ЭСП;
- обеспечивать функционирование и безопасность Платежной системы;
- обеспечивать получение и обработку электронных сообщений, содержащих Распоряжения Участников 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;
- осуществлять обмен нефинансовыми сообщениями с Участниками по всем направлениям их деятельности в Системе.

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

4.2.1.6. Предоставлять информацию о своей деятельности в рамках Системы по запросам Оператора, в том числе внутренние документы и договоры, в сроки и объеме, устанавливаемые в запросе Оператора. В случае внесения изменений в учредительные документы, а также при изменении любых других данных Операционного центра, сведения о которых предоставлены Оператору, предоставить обновленные документы и информацию не позднее 5 (пяти) рабочих дней с даты внесения в них изменений, если более короткий срок не установлен Оператором либо не вытекает из обычаев делового оборота и(или) требований безопасности.

4.2.1.7. Не приостанавливать (прекращать) в одностороннем порядке оказание услуг платежной инфраструктуры Участникам и их Клиентам.

4.2.1.8. Обеспечивать защиту информации при обмене электронными сообщениями между Участниками, между Участниками и их Клиентами, Платежным клиринговым центром, Расчетным центром, между Платежным клиринговым центром и Расчетным центром.

4.2.1.9. Реализовать процессы выявления и идентификации риска информационной безопасности (далее – «Риск ИБ») в отношении объектов своей информационной инфраструктуры.

4.2.1.10. Проводить работы по выявлению и анализу Риска ИБ при переводе денежных средств в рамках Системы.

4.2.1.11. Реализовывать мероприятия, направленные на противодействие осуществлению переводов денежных средств без добровольного согласия клиента.

4.2.1.12. Нести ответственность за реальный действительный ущерб, причиненный Участникам, Платежному клиринговому центру и Расчетному центру вследствие неоказания (ненадлежащего оказания) операционных услуг.

4.2.2. Операционный центр вправе:

4.2.2.1. Оказывать операционные услуги в рамках других платежных систем.

4.2.2.2. В случае обнаружения неисправностей, ошибок или сбоев в работе программных и/или аппаратных средств, задействованных в обеспечении функционирования Системы, а также в профилактических целях и целях предотвращения несанкционированного доступа к Системе – приостанавливать работу программных и аппаратных средств.

4.2.2.3. С предварительного согласования с Оператором определять и вносить изменения в технические условия подключения и функционирования Системы.

4.2.2.4. Привлекать третьих лиц для исполнения принятых на себя обязанностей, оставаясь ответственным за их действия.

4.2.2.5. При осуществлении иных действий, связанных с использованием информационно-коммуникационных технологий, необходимых для функционирования Платежной системы, оказывать:

(а) услуги по информационно-технологическому взаимодействию между кредитной организацией, являющейся Субъектом Правил (далее для целей настоящего пункта – «Кредитная организация»), и Получателем-юридическим лицом/индивидуальным предпринимателем, в целях осуществления переводов денежных средств в пользу такого Получателя-юридического лица/индивидуального предпринимателя в рамках Платежной системы, в том числе предоставлять технологии передачи информации при взаимодействии Кредитной организации с Получателем-юридическим лицом/индивидуальным предпринимателем, организовывать каналы связи в целях обмена сообщениями между Кредитной организацией и Получателем-юридическим лицом/индивидуальным предпринимателем, обеспечивать маршрутизацию электронных сообщений, получать от Кредитной организации или Получателя-юридического лица/индивидуального предпринимателя информацию о результатах проведения операции;

(б) услуги по сбору и передаче Участнику информации, необходимой для формирования Распоряжения Отправителя на осуществление перевода денежных средств, в том числе путем предоставления необходимых ресурсов (веб-страниц, приложений и т.п.) и поддержке их надлежащего функционирования;

(в) иные услуги, связанные с использованием информационного-коммуникационных технологий, необходимые для функционирования Платежной системы.

4.3. Права и обязанности Платежного клирингового центра

4.3.1. **Платежный клиринговый центр обязан**:

4.3.1.1. Осуществлять свою деятельность в соответствии с настоящими Правилами и на основании договоров об оказании услуг платежного клиринга, заключаемых с Оператором (в случае привлечения Оператором Платежного клирингового центра), с Операторами УПИ, указанными Оператором, и Участниками (в случае привлечения Оператором Платежного клирингового центра).

4.3.1.2. Выполнять следующие функции:

- выполнять процедуры приема к исполнению Распоряжений Участников об осуществлении перевода денежных средств, включая проверку соответствия Распоряжений Участников установленным требованиям, определять достаточность денежных средств для исполнения Распоряжений Участников Системы;
- передавать Расчетному центру от имени Участников подлежащие исполнению Распоряжения Участников;
- определять платежные клиринговые позиции по каждой из валют расчета;
- формировать и направлять Отчеты Участникам на основании поступивших Распоряжений Клиентов и Распоряжений Участников, а также об исполнении Распоряжений с целью извещения (подтверждения) Участников об исполнении Распоряжений согласно Временному регламенту;
- формировать и направлять в ЦПКК Отчет по операциям ЦПКК на основании поступивших Распоряжений Клиентов и Распоряжений Участников согласно Временному регламенту (по необходимости);

- по результатам платежного клиринга формировать и направлять Расчетному центру для исполнения от имени Участников, итоговую сумму принятых за предыдущий операционный день Распоряжений Участников в виде Реестра для осуществления расчета по Счетам Участников и Счетам ЦПКК (по необходимости);
- рассчитывать вознаграждения (комиссии), причитающиеся Субъектам в соответствии с Тарифами и заключенными договорами;
- обеспечивать выполнение требований безопасности в Платежной системе в соответствии с Правилами.

4.3.1.3. При предоставлении услуг платежного клиринга 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, а также обеспечивать защиту информации при осуществлении следующих операций:

- выполнение процедур приема к исполнению электронных сообщений Участников, включая проверку соответствия электронных сообщений Участников, определение достаточности денежных средств для исполнения электронных сообщений Участников и определение платежных клиринговых позиций;
- передача Расчетному центру для исполнения электронных сообщений Платежного клирингового центра, принятых электронных сообщений Участников;
- направление Участникам извещений (подтверждений), касающихся приема к исполнению электронных сообщений Участников, а также передача извещений (подтверждений), касающихся исполнения электронных сообщений Участников.

4.3.1.4. Реализовать процессы выявления и идентификации Риска ИБ в отношении объектов своей информационной инфраструктуры.

4.3.1.5. Проводить работы по выявлению и анализу Риска ИБ при переводе денежных средств в рамках Системы.

4.3.1.6. Реализовывать мероприятия, направленные на противодействие осуществлению переводов денежных средств без добровольного согласия клиента.

4.3.1.7. Предоставлять информацию о своей деятельности в рамках Системы по запросам Оператора, в том числе внутренние документы и договоры, в сроки и объеме, устанавливаемые в запросе Оператора. В случае внесения изменений в учредительные документы, а также при изменении любых других данных Платежного клирингового центра, сведения о которых предоставлены Оператору, предоставить обновленные документы и информацию не позднее 5 (пяти) рабочих дней с даты внесения в них изменений, если более короткий срок не установлен Оператором либо не вытекает из обычаев делового оборота и(или) требований безопасности.

4.3.1.8. Не приостанавливать (прекращать) в одностороннем порядке оказание услуг платежной инфраструктуры Участникам и Клиентам.

4.3.1.9. Нести ответственность за убытки, причиненные Участникам Платежной системы и Расчетному центру вследствие неоказания (ненадлежащего оказания) услуг платежного клиринга. Правилами или договором об оказании услуг платежного клиринга ответственность Платежного клирингового центра за убытки может быть ограничена размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежного клиринга.

4.3.1.10. При выполнении функций ЦПКК:

- осуществлять свою деятельность в соответствии с договорами, заключенными с Оператором;
- обладать денежными средствами, достаточными для исполнения своих обязательств по переводу денежных средств, либо обеспечивать исполнение своих обязательств, в размере наибольшего обязательства, по которому ЦПКК становится плательщиком, за предыдущий

операционный день/дни (в соответствии с порядком, предусмотренным Временным регламентом);

- ежедневно осуществлять контроль за рисками неисполнения (ненадлежащего исполнения) Участниками своих обязательств по переводу денежных средств, применять в отношении Участников, анализ финансового состояния которых свидетельствует о повышенном риске, ограничительные меры, включая установление максимального размера платежной клиринговой позиции, и предъявлять требования о повышенном размере обеспечения исполнения обязательств Участников по переводу денежных средств;
- при поступлении запроса от Оператора предоставлять выписку по Счету ЦПКК, отражающую операции, осуществляемые в рамках Платежной системы.

4.3.2. **Платежный клиринговый центр имеет право:**

4.3.2.1. Оказывать услуги платежного клиринга в рамках других платежных систем.

4.3.2.2. Отказать в приеме Распоряжения Участника в случае, если оно не прошло проверку в соответствии с Правилами или действующим законодательством.

4.3.2.3. Привлекать третьих лиц, оставаясь ответственным за их действия.

4.3.2.4. При наличии правоспособности, соответствующей Федеральному закону №161-ФЗ, выполнять функции ЦПКК.

4.4. **Права и обязанности Расчетного центра**

4.4.1. **Расчетный центр обязан**:

4.4.1.1. Осуществлять свою деятельность в соответствии с настоящими Правилами, договором об оказании услуг Расчетного центра и на основании договоров банковского счета, заключаемых с Участниками.

4.4.1.2. Исполнять поступившие от Платежного клирингового центра Распоряжения Участников посредством списания и зачисления денежных средств по Счетам Участников и (или) по Счету ЦПКК.

4.4.1.3. Осуществлять свою деятельность ежедневно по рабочим дням на основании поступивших от Платежного клирингового центра Распоряжений Участников в форме Реестра. В Реестр включаются также суммы, подлежащие списанию со Счета (зачислению на Счет) ЦПКК.

4.4.1.4. Предоставлять Платежному клиринговому центру данные по остаткам, изменению остатков денежных средств на Счетах Участников для формирования Лимитов Участников.

4.4.1.5. Направлять Оператору отчеты о своевременности и полноте исполнения Участниками своих обязательств, способствовать выявлению фактов нарушения Участниками своих обязательств.

4.4.1.6. На основании уведомлений Оператора о приостановке обслуживания (блокировке) Участника Расчетный центр производить приостановку проведения расчетов в Платежной системе.

4.4.1.7. 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, а также обеспечивать защиту информации при исполнении поступивших от Платежного клирингового центра электронных сообщений Платежного клирингового центра и (или) Участников посредством списания и зачисления денежных средств по Счетам Участников и (или) по Счету ЦПКК.

4.4.1.8. Реализовать процессы выявления и идентификации Риска ИБ в отношении объектов своей информационной инфраструктуры.

4.4.1.9. Проводить работы по выявлению и анализу Риска ИБ при переводе денежных средств в рамках Системы.

4.4.1.10. Не приостанавливать (прекращать) в одностороннем порядке оказание услуг платежной инфраструктуры Участникам и Клиентам.

4.4.1.11. Предоставлять Оператору информацию об открытых/закрытых Участнику и(или) ЦПКК Счетах и иную информацию, связанную со Счетами Участников, используемыми ими для расчетов в рамках Платежной системы, не позднее 3 (трех) рабочих дней с даты наступления соответствующего события, если иной срок не будет установлен договором между Оператором и Расчетным центром.

4.4.1.12. В случае осуществления расчетов в Платежной системе с использованием нескольких Расчетных центров, осуществлять взаимодействие с другим расчетным центром на основании отдельных договоров с Оператором и (или) с другим расчетным центром (при необходимости).

4.4.1.13. Реализовывать мероприятия, направленные на противодействие осуществлению переводов денежных средств без добровольного согласия клиента.

4.4.1.14. Предоставлять информацию о своей деятельности в рамках Системы по запросам Оператора, в том числе внутренние документы и договоры, в сроки и объеме, устанавливаемые в запросе Оператора. В случае внесения изменений в учредительные документы, а также при изменении любых других данных Расчетного центра, сведения о которых предоставлены Оператору, предоставить обновленные документы и информацию не позднее 5 (пяти) рабочих дней с даты внесения в них изменений, если более короткий срок не установлен Оператором либо не вытекает из обычаев делового оборота и(или) требований безопасности.

4.4.1.15. Обеспечивать бесперебойность оказания расчетных услуг, предоставляемых Субъектам Системы, а также организовывать управление рисками в части полномочий, делегированных ему Оператором.

4.4.1.16. При поступлении запроса от Оператора при наличии предварительного согласия Участника и(или) ЦПКК предоставлять Оператору выписку по Счету Участника и(или) Счету ЦПКК.

4.4.1.17. В случае выполнения Расчетным центром функций Платежного клирингового центра, являющегося ЦПКК, обеспечивать выполнение требований, предусмотренных пп. 4.3.1.10 Правил.

4.4.2. **Расчетный центр имеет право**:

4.4.2.1. Запрашивать у Оператора и (или) Участников информацию об операциях Клиентов в рамках осуществления контроля исполнения Участниками, находящимися у него на обслуживании, требований, предусмотренных законодательством о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

4.4.2.2. Оказывать расчетные услуги в рамках других платежных систем.

4.4.2.3. Осуществлять анализ финансового состояния Участника в целях определения возможности предоставления ему расходного Лимита и (или) кредита для целей увеличения доступного Лимита Участника.

4.4.2.4. Совмещать свои функции с функциями Участника и(или) ПКЦ, в том числе для выполнения последним функций ЦПКК.

4.5. Права и обязанности Участника

4.5.1. **Участник обязан:**

4.5.1.1. Самостоятельно обеспечить техническое и технологическое взаимодействие с Операционным центром и Платежным клиринговым центром Платежной системы для получения информации о финансовых сообщениях в соответствии с особенностями осуществления платежного клиринга, предусмотренного Правилами.

4.5.1.2. Представлять Оператору документы и информацию в соответствии с требованиями Правил. По запросу Оператора предоставлять в порядке и сроки, указанные в таком запросе, внутренние документы, справки, информацию, договоры и иные документы, касающиеся исполнения обязательств Участником Правил Платежной системы и действующего законодательства, а также

необходимые Оператору для исполнения обязанностей, предусмотренных Правилами и действующим законодательством.

4.5.1.3. Предоставлять Оператору достоверную информацию для регистрации в Системе (интеграции в Систему) и осуществления деятельности в качестве Участника; сообщать Оператору перечень типов Переводов, которые не могут быть совершены им в рамках Системы в силу требований законодательства страны инкорпорации Участника.

4.5.1.4. Оплачивать услуги, предоставляемые Оператором, Операторами УПИ, а также осуществлять расчеты в сроки и в порядке, определенные Правилами.

4.5.1.5. В случае если он выступает Прямым участником – открыть Счет/Счета в Расчетном центре, определенном Оператором Платежной системы.

4.5.1.6. В случае если он выступает Косвенным участником – открыть Счет у Прямого участника, за исключением случаев, указанных в п. 3.2.2.2 Правил.

4.5.1.7. В случае поступления запроса от Оператора в целях осуществления сверки расчетов предоставить сведения об операциях по Счету, отрытому для осуществления расчетов в Платежной системе в форме выписки или в иной форме, согласованной с Оператором. Прямой участник вправе предоставить Расчетному центру, а Косвенный участник – Прямому участнику согласие на предоставление Оператору сведений об операциях по Счету в форме выписки по Счету Участника в рамках договора банковского счета, открываемого Прямым участником в Расчетном центре, а Косвенным участником – у Прямого участника.

4.5.1.8. Контролировать достаточность денежных средств на Счетах в Расчетном центре/у Прямого участника для формирования Лимита Участника.

4.5.1.9. Предоставить Расчетному центру Системы/Прямому участнику право на списание денежных средств со своих Счетов, открытых в соответствующем Расчетном центре/у Прямого участника, без дополнительного распоряжения Прямого участника/Косвенного участника соответственно на условиях заранее данного акцепта при предъявлении Оператором Системы требования о списании.

4.5.1.10. Перечислить на Счет, открытый в Расчетном центре/у Прямого участника необходимую сумму денежных средств для формирования Лимита Участника до начала осуществления переводов в рамках ПС, если иное не будет согласовано с Оператором. Условия расчетов между Прямым и Иным Косвенным участником (в случае, если Прямой участник осуществляет расчеты с Косвенным участником без открытия Счета у Прямого участника), регулируются договором между Прямым и Косвенным участником.

4.5.1.11. Самостоятельно определять сумму денежных средств, перечисляемую на свой Счет в Расчетном центре/у Прямого участника для формирования Лимита Участника.

4.5.1.12. Своевременно и в полном объеме исполнять свои денежные обязательства перед другими Участниками.

4.5.1.13. Осуществлять расчеты по операциям, совершенным с использованием Системы, на основании Отчетов Участников, предоставленных Платежным клиринговым центром.

4.5.1.14. Контролировать в соответствии с действующим законодательством исполнение Партнерами, БПА своих обязательств по перечислению собранных денежных средств Клиентов, выявлять факты нарушения Партнерами, БПА своих обязательств и настоящих Правил, и самостоятельно осуществлять действия по истребованию неполученных в срок денежных средств с Партнеров, БПА. Прямой участник осуществляет вышеперечисленные действия по отношению к Косвенному участнику.

4.5.1.15. Нести финансовую ответственность перед Оператором и Субъектами Системы за действия Косвенных участников, Партнеров, БПА/БПСА в рамках их деятельности в Системе.

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

4.5.1.17. Обеспечивать защиту информации при осуществлении переводов денежных средств в соответствии с Правилами и требованиями, установленными законодательством Российской Федерации, в том числе реализовывать мероприятия, направленные на противодействие осуществлению переводов денежных средств без добровольного согласия Клиента.

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

4.5.1.19. Реализовать процессы выявления и идентификации Риска ИБ в отношении объектов своей информационной инфраструктуры.

4.5.1.20. Проводить работы по выявлению и анализу Риска ИБ при переводе денежных средств в рамках Системы.

4.5.1.21. Осуществлять идентификацию Клиентов в соответствии с требованиями законодательства страны инкорпорации Участника и настоящих Правил.

4.5.1.22. Обеспечить выполнение БПА требований по идентификации Клиентов в соответствии с требованиями законодательства Российской Федерации и настоящих Правил (в случае наделения привлеченных БПА обязанностями по идентификации Клиентов).

4.5.1.23. В случае внесения изменений в учредительные документы, а также при изменении любых других данных Участника, его Партнеров и(или) БПА/БПСА, сведения о которых предоставлены Оператору, предоставить обновленные документы и информацию не позднее 5 (пяти) рабочих дней с даты внесения в них изменений, если более короткий срок не установлен Оператором либо не вытекает из обычаев делового оборота и(или) требований безопасности.

4.5.2. **Участник имеет право:**

4.5.2.1. Участвовать в других платежных системах.

4.5.2.2. Присоединиться к настоящим Правилам и стать Участником Системы при условии соответствия критериям участия в Системе.

4.5.2.3. Пользоваться всеми технологическими возможностями Системы.

4.5.2.4. Участвовать в информационном и технологическом взаимодействии в Системе с даты начала участия в Системе.

4.5.2.5. Привлекать Косвенных участников и Партнеров при условии соблюдения ими Правил Платежной системы.

4.5.2.6. Привлекать БПА в целях выполнения обязанностей в соответствии с законодательством Российской Федерации (прием от физических лиц наличных денежных средств, выдача физическому лицу наличных денежных средств, иные операции, предусмотренные Федеральным законом №161-ФЗ), предоставлять привлеченным БПА возможность привлекать БПСА при условии соблюдения этими БПА и БПСА настоящих Правил.

4.5.2.7. Самостоятельно устанавливать операционное (рабочее) время, в течение которого Участник осуществляет обслуживание Клиентов в головном офисе, филиалах и отделениях Участника, а также дистанционное обслуживание Клиентов.

4.5.2.8. Осуществлять мероприятия, направленные на продвижение своих услуг в рамках Системы.

4.5.2.9. Получать от Оператора Отчеты в связи с совершенными в Системе операциями по переводу денежных средств.

4.5.2.10. Привлекать третьих лиц для обеспечения информационного взаимодействия в Системе, оставаясь ответственным за действия (бездействия) таких привлеченных лиц, как за свои собственные.

4.6. Особенности взаимодействия с Участниками-Иностранными поставщиками платежных услуг

4.6.1. В рамках расширения географии и предоставляемых услуг Участникам Платежной системы МАРЛИН, Оператор от своего имени вправе заключать договоры с Иностранными поставщиками платежных услуг. Оформление взаимоотношений с Иностранными поставщиками платежных услуг может осуществляться в форме Договора участия в Платежной системе.

4.6.2. Расчеты с Участниками Платежной системы МАРЛИН в рамках взаимодействия с Иностранными поставщиками платежных услуг обеспечивает Расчетный центр.

4.6.3. Особенности взаимодействия с Иностранным поставщиком платежных услуг, предоставляющих ЭСП Клиентам, определяются с учетом требований, предусмотренных Федеральным законом №161-ФЗ.

4.6.4. На дату утверждения настоящей редакции Правил договоры с Иностранными поставщиками платежных услуг, предоставляющими иностранным Клиентам ЭСП для их приема на территории Российской Федерации, отсутствуют.

4.7. Функции Банковского платежного агента

4.7.1. БПА осуществляет свою деятельность в Системе на основании договора с Участником. БПА не является напрямую субъектом Системы.

4.7.2. БПА участвует в информационном и технологическом взаимодействии в Системе в соответствии с настоящими Правилами и договором, заключенным с Участником.

4.7.3. Для выполнения своих функций БПА по требованию Участника открывает у него расчетный счет, необходимый для обеспечения своевременного проведения расчетов с Участником в порядке и по форме, которые установлены Участником.

4.7.4. На основании договора с Участником БПА от имени Участника может выполнять следующие действия:

- принимать от Клиентов-физических лиц наличные денежные средства;
- выдавать Клиентам- физическим лицам наличные денежные средства;
- обеспечивать предоставление Клиентам-физическим лицам ЭСП и (или) возможность их использования;
- осуществлять идентификацию или упрощенную идентификацию Клиента - физического лица в целях осуществления перевода денежных средств без открытия банковского счета, а также предоставления клиенту - физическому лицу ЭСП;
- выполнять иные действия, предусмотренные Федеральным законом №161-ФЗ.

4.7.5. БПА сдает наличные денежные средства, полученные от Клиентов-физических лиц, в полном объеме на свой специальный банковский счет, и проводит расчеты с Участником в порядке, предусмотренном договором с ним.

4.7.6. БПА в соответствии с условиями договора с Участником может привлекать БПСА для осуществления отдельных операций в Системе при условии соблюдения требований о привлечении БПСА, установленных Федеральным законом №161-ФЗ.

4.7.7. БПА обязан при совершении операции подтверждать принятие (выдачу) наличных денежных средств путем выдачи (направления) кассового чека.

4.7.8. БПА поддерживает работоспособность своего оборудования и корректную настройку своего программного обеспечения, своевременно выполняет необходимые для устранения выявленных

неполадок работы. БПА вправе использовать программное обеспечение, предоставляемое Системой, в целях осуществления переводов только через Систему.

4.7.9. БПА обязан исключить доступ к информации сотрудников БПА, которые непосредственно не связаны с работой в Системе.

4.7.10. БПА, в случае открытия у Участника расчетного счета, необходимого для обеспечения исполнения обязательств по своевременному проведению расчетов, по требованию Участника предоставляет последнему право списания со счета БПА денежных средств, принятых от Клиентов на основании Отчетов Участника, подготовленных Оператором.

4.7.11. В месте осуществления операций БПА (БПСА) до начала осуществления каждой операции физическим лицам должна предоставляться следующая информация:

- адрес места осуществления операций БПА/БПСА;
- наименование и место нахождения Участника и БПА/БПСА, а также их идентификационные номера налогоплательщика;
- номер лицензии Участника на осуществление банковских операций;
- реквизиты договора между Участником и БПА, а также реквизиты договора между БПА и БПСА (в случае его привлечения);
- размер вознаграждения, уплачиваемого Клиентом в виде общей суммы, включающей в том числе, вознаграждение БПА/БПСА в случае его взимания;
- способы подачи претензий, заявлений и порядок их рассмотрения;
- номера телефонов Информационно-справочного центра, Участника, БПА и БПСА (в случае его привлечения).

4.7.12. БПА участвует в рассмотрении обращений Клиентов по вопросам, связанным с осуществлением операций.

4.7.13. БПА в полном объеме несет имущественные риски по возмещению возникших у Участников убытков в результате действий БПА.

4.7.14. БПА в полном объеме несет ответственность, в том числе и финансовую, за действия привлеченных БПСА.

4.8. Партнеры Платежной системы МАРЛИН

4.8.1. Участник вправе в целях осуществления Переводов привлекать Партнеров в Систему. Партнер не является напрямую субъектом Системы.

4.8.2. Партнеры осуществляют переводы денежных средств в соответствии с соглашениями, заключенными с Участниками с учетом требований настоящих Правил. Для заключения соглашения с Участником Партнер предоставляет пакет документов, запрашиваемый Участником. Необходимость открытия Партнером корреспондентского счета у Участника определяется по соглашению между Участником и Партнером.

4.8.3. Соглашение между Участником и Партнером заключается путем подписания сторонами документа на бумажном носителе или в электронной форме с использованием усиленных квалифицированных электронных подписей сторон. Участник несет ответственность перед Оператором за соблюдение Партнером условий настоящих Правил. Договор Участника с Партнером может быть заключен при участии Оператора.

4.8.4. Оператор Системы на период сотрудничества Партнера с Участником может обеспечивать обмен электронными сообщениями между Участником и Партнером по операциям их Клиентов, а также может предоставлять Партнерам на условиях неисключительной лицензии право использования ПО Системы для целей предоставления Услуг Системы Клиентам Партнеров. При прекращении сотрудничества сторон Оператор прекращает обмен электронными сообщениями

между Участником и Партнером, а в случае предоставления Партнеру неисключительного права на использование ПО Системы, оно автоматически прекращается в последний день действия соглашения между Участником и Партнером. Участник обязан уведомить Оператора Системы о прекращении сотрудничества с Партнером не позднее чем за 3 (три) рабочих дня до даты расторжения соглашения.

4.8.5. Все имущественные и неимущественные права, включая исключительное право на ПО Системы и на все его копии, принадлежат Оператору Системы. Партнер не вправе каким-либо образом самостоятельно изменять или расширять ПО Системы.

4.8.6. Заключаемые соглашения определяют порядок взаимодействия Участников, в том числе Оператора, и Партнеров. В случае если то или иное положение не оговорено такими соглашениями, Партнеры руководствуются Правилами Платежной системы, используемыми в соответствующих случаях Участниками.

4.8.7. В соглашениях Участника и Партнера, при необходимости, (при невозможности руководствоваться Правилами Платежной системы) прописываются индивидуальные размеры и порядок оплаты комиссионного вознаграждения, причитающегося Участнику, в том числе Оператору, и Партнеру, условия осуществления расчетов и порядок электронного документооборота, особенности отправки/ выплаты переводов денежных средств в адрес/ от Клиентов Партнера, в том числе ограничения Партнера по суммам переводов денежных средств при их наличии, валюта выплаты переводов денежных средств Партнером и другие особенности взаимоотношений.

4.8.8. Партнер обязан:

а) доводить до Клиентов порядок осуществления Переводов, информацию о размере комиссии за Перевод, а также иную информацию о работе Партнера до фактического внесения/списания денежных средств Клиента;

б) самостоятельно подготовить для своих сотрудников внутренние инструкции по работе с ПО Системы с Клиентами, соответствующие законодательству государства инкорпорации Партнера (при необходимости);

в) информировать Участника о возникновении обстоятельств, временно препятствующих приему и/или выплате Переводов в пунктах обслуживания Партнера;

г) принимать меры, исключающие несанкционированный ввод и передачу информации о Переводах от имени Партнера;

д) хранить документы, представляемые Клиентами при осуществлении Переводов, вести архивы электронных уведомлений и поручений не менее 5 (пяти) лет, представлять Участнику полные, точные и разборчивые копии документов, касающихся Переводов, в течение 5 (пяти) дней после получения соответствующего запроса.

4.8.9. Партнер обязуется предоставлять Участнику отчетность, предусмотренную законодательством, а также иные документы и информацию, связанные с выполнением обязательств по соглашению, по требованию Участника в установленные в запросе сроки. Непредставление Партнером отчетов, документов или информации в установленные сроки является основанием для приостановления действия сотрудничества Участника и Партнера (в том числе по требованию Оператора Системы) в одностороннем порядке на период, в течение которого отчетность, документы или информация не предоставлены.

4.8.10. Наступление окончательности, порядок и условия внесения изменений или аннулирования переводов денежных средств, направленных для выплаты Получателю Партнером, имеют следующие особенности:

4.8.10.1. окончательность перевода денежных средств наступает в момент зачисления денежных средств на счет Участника, чьим клиентом является Партнер;

4.8.10.2. возможность или невозможность внесения изменений определяется Партнером на основании запроса, полученного от Оператора Системы. При получении от Партнера информации о невозможности внесения изменений в перевод денежных средств

Оператор Системы незамедлительно извещает Участника о данном факте по Согласованным каналам связи;

4.8.10.3. возможность или невозможность осуществления возврата перевода денежных средств определяется Партнером на основании запроса, полученного от Оператора Системы. При получении от Партнера информации о невозможности возврата перевода денежных средств Оператор Системы незамедлительно извещает Участника о данном факте по Согласованным каналам связи.

4.8.11. Порядок и условия внесения изменений или аннулирования переводов денежных средств, принятых Партнером от Отправителя, а также порядок сверки расчетов по совершенным операциям аналогичны порядку и условиям, установленным настоящими Правилами для Участников.

4.8.12. Партнер осуществляет обслуживание Клиентов в соответствии с условиями, изложенными в разделе 6 Правил. Существующие особенности отправки/выплаты, внесения изменений или осуществления возврата переводов денежных средств в пользу Клиентов Партнеров, основанные, в том числе на положениях законодательства страны местонахождения Партнера, Оператор Системы доводит до сведения Участников Платежной системы по Согласованным каналам связи. Доведение указанных особенностей до сведения Клиентов - физических лиц Оператор Системы осуществляет путем размещения их на официальном сайте Оператора Системы в информационно-телекоммуникационной сети Интернет по адресу: www.marlinpay.ru.

4.8.13. Обязательства Партнеров учитываются в платежной клиринговой позиции Участника, с которым у Партнера заключено соответствующее соглашение.

4.8.14. Партнер обязан обеспечить защиту информации при оказании Клиентам услуг Платежной системы МАРЛИН в соответствии с требованиями раздела 10 Правил, а также выполнять иные требования Правил, связанные с управлением рисками и бесперебойностью работы в Платежной системе.

4.8.15. Партнер обязан хранить данные об операциях и Клиентах не менее 5 (пяти) лет с даты осуществления операции, если более длительный срок не определен в соглашении между Партнером и Участником. Партнер обязан предоставлять Участнику и(или) Оператору Системы запрашиваемые им сведения, касающиеся деятельности Партнера в рамках Платежной системы, не позднее 5 (пяти) рабочих дней с даты получения запроса от Участника и(или) Оператора Системы.

4.8.16. С момента прекращения участия Участника в Платежной системе прекращается и деятельность его Партнеров.

5. УЧАСТИЕ В ПЛАТЕЖНОЙ СИСТЕМЕ

5.1. Виды и критерии участия в Платежной системе

5.1.1. Платежная система предусматривает:

- Прямое участие (Прямые участники), которое предполагает открытие Участниками банковских счетов в Расчетном центре Системы;
- Косвенное участие (Косвенные участники), которое предполагает открытие Участниками банковских счетов у Прямых участников либо заключение с Прямым участником отдельного договора об осуществлении расчетов в рамках Платежной системы в соответствии с требованиями, изложенными в пп. 3.2.2.2 Правил.

5.1.2. Участниками Системы могут являться операторы по переводу денежных средств (включая Операторов электронных денежных средств), международные финансовые организации, иностранные центральные (национальные) банки, иностранные банки (иностранные кредитные организации), Иностранные поставщики платежных услуг.

5.1.2.1. Прямыми участниками Платежной системы могут являться только операторы по переводу денежных средств (включая Операторов электронных денежных средств), международные финансовые организации, иностранные центральные (национальные) банки, иностранные банки (иностранные кредитные организации).

5.1.2.2. Косвенными участниками Платежной системы могут являться операторы по переводу денежных средств (включая Операторов электронных денежных средств), международные финансовые организации, иностранные центральные (национальные) банки, иностранные банки (иностранные кредитные организации), Иностранные поставщики платежных услуг.

5.1.3. Критерии прямого участия в Системе:

- соответствие общим критериям участия в Системе, указанным в пункте 5.1.5 Правил;
- успешное прохождение Участником процедур проверок Расчетным центом на соответствие внутренним правилам и политикам открытия счетов, в том числе проверок по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризму;
- наличие банковского счета (счетов) в Расчетном центре Системы;
- наличие Договора участия в Системе, заключенного с Оператором;
- наличие договоров с Операционным центром и Платежным клиринговым центром (в случае их привлечения Оператором);
- соблюдение настоящих Правил, Договора участия в Системе, договоров с Операционным центром и Платежным клиринговым центром (в случае их привлечения Оператором), иных документов Оператора, устанавливающих права и обязанности Субъектов Системы, в том числе в рамках БФПС.

5.1.4. Критерии косвенного участия в Системе:

- соответствие общим критериям участия в Системе, указанным в пункте 5.1.5 Правил;
- успешное прохождение Участником процедур проверок, осуществляемых Прямым участником на соответствие внутренним правилам и политикам открытия счетов (в случае их открытия) или заключения иных видов договоров, предусматривающих взаиморасчеты с Иными Косвенными участниками, в том числе проверок по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризму;
- наличие банковского счета (счетов), открытого у Прямого участника Системы или заключение отдельного договора с Иным Косвенным участником об осуществлении взаиморасчетов по операциям, осуществляемым в рамках Системы;

- наличие Договора участия в Системе, заключенного с Оператором;
- наличие договоров с Операционным центром и Платежным клиринговым центром (в случае их привлечения Оператором);
- соблюдение настоящих Правил, Договора участия в Системе, договоров с Операционным центром и Платежным клиринговым центром (в случае их привлечения Оператором), иных документов Оператора, устанавливающих права и обязанности Субъектов Системы, в том числе в рамках БФПС.

5.1.5. Общие критерии участия в Системе:

- общая финансовая устойчивость;
- наличие технической возможности регистрации в Системе (интеграции в Систему);
- обеспечение защиты информации, в том числе защиты персональных данных в сети Участника и при работе в Системе;
- готовность предоставления Участником Оператору периодической отчетности о работе в Системе, включая информацию по рискам и информационной безопасности;
- наличие необходимых лицензий на осуществление деятельности по переводу денежных средств в соответствии с требованиями законодательства Российской Федерации или законодательства страны инкорпорации Участника;
- обеспечение банковской тайны;
- выполнение Участником требований по противодействию отмыванию доходов, полученных преступным путем, и финансированию терроризма, установленных законодательством Российской Федерации или законодательства страны инкорпорации Участника;
- выполнение требований, предусмотренных п. 5.3 Правил;
- отсутствие иных обстоятельств, препятствующих или существенно ограничивающих возможности взаимодействия Участников с Субъектами Системы или вызывающих коллизии применимого законодательства и (или) угрожающих стабильности работы Системы.

5.2. Общие условия и порядок присоединения Участника к Системе

5.2.1. Присоединение Участника к Системе осуществляется путем присоединения к настоящим Правилам, которые могут быть приняты Участником Системы не иначе как в целом, путем заключения Договора участия в порядке, установленном Правилами.

5.2.2. Подписание Участником Договора участия означает безусловное признание Правил и применение их в качестве документа, регулирующего отношения сторон в рамках участия в Системе. Каждый из Участников Системы гарантирует, что обладает необходимой правоспособностью, всеми правами и полномочиями, необходимыми и достаточными для присоединения к Системе и исполнения обязательств в соответствии с условиями Правил.

5.2.3. Лицо, намеревающееся стать Участником, должно представить непосредственно Оператору заявление по форме Приложения №1 к настоящим Правилам. Косвенный участник, одновременно с заявлением, предоставляет согласие Прямого участника на установление договорных взаимоотношений с Косвенным участникам в рамках Системы. В контексте настоящего раздела Правил лицо, намеревающееся стать Участником Системы, именуется как «Заявитель».

5.2.4. Вместе с заявлением Заявитель предоставляет пакет документов, определенный Оператором.

5.2.5. Оператор анализирует представленный Заявителем пакет документов, принимает решение о возможности сотрудничества (об отказе в сотрудничестве) с ним в качестве Участника и информирует контактное лицо Заявителя, указанное в заявлении, о принятом решении.

5.2.6. В случае принятия Оператором положительного решения о сотрудничестве Заявитель обращается в Расчетный центр/к Прямому участнику для заключения договора банковского счета. Иные Косвенные участники обращаются к Прямому участнику для заключения договора об осуществлении взаиморасчетов по операциям, осуществляемым в рамках Системы. Перечень документов, предоставляемых в Расчетный центр/Прямому участнику для открытия банковского счета или заключения договора об осуществлении взаиморасчетов по операциям, осуществляемым в рамках Системы, а также форма указанных договоров определяется Расчетным центром или Прямым участником соответственно. Условия договоров, предусмотренных настоящим пунктом, не должны противоречить настоящим Правилам. В случае любых несоответствий между настоящими Правилами и договором Расчетного центра с Участником или договором Прямого участника с Косвенным участником, преимущественную силу имеют положения Правил.

5.2.7. Оператор получает информацию от Расчетного центра (Прямого участника) об открытии Заявителю банковского счета. Прямой участник информирует Оператора о заключении договора с Иным Косвенным участником, регламентирующего порядок взаимоотношений Сторон при осуществлении операций в Системе.

5.2.8. Оператор подписывает Договор участия и направляет его Заявителю.

5.2.9. Оператор осуществляет регистрацию Участника в Системе и присваивает ему код Участника, который позволяет однозначно установить Участника и вид его участия в Платежной системе. Код Участника является уникальным, состоит из 6 (шести) символов в длину. Присвоение кода Участника осуществляется по шаблону XYYYYY, где X – категория Участника (Прямой или Косвенный), YYYYY – его номер. Одновременно с присвоением кода проводится техническое тестирование работоспособности Участника.

5.2.10. Датой начала участия Участника в Платежной системе является подписание Оператором и Участником акта технической готовности, подтверждающего готовность Участника к оказанию Услуг Системы.

5.2.11. Порядок регистрации Участником привлеченных им лиц (Партнеров, БПА, БПСА):

5.2.11.1. Оказание Услуг Системы Партнером и(или) БПА осуществляется на основании договора с Участником, на основании которого Партнер и(или) БПА от имени Участника осуществляют действия в Системе.

5.2.11.2. На основании подписанных договоров между Участником и Партнером и(или) Участником и БПА, Участник направляет Оператору заявление о регистрации Партнера и(или) БПА в Системе. В отдельных случаях Оператор может требовать от привлеченного лица заключения дополнительных договоров, предусматривающих возможность использования специализированного программного обеспечения для осуществления отдельных видов операций.

5.2.11.3. Оператор на основании заявления Участника осуществляет регистрацию Партнера и(или) БПА в ПО Системы с присвоением соответствующих идентификаторов.

5.2.11.4. Оказание Услуг Системы БПСА осуществляется на основании договора между БПА и БПСА, на основании которого БПСА от имени Участника осуществляет действия в Системе в соответствии с Правилами.

5.2.11.5. На основании подписанного договора между БПА и БПСА, БПА направляет Участнику заявление о регистрации БПСА. Участник, в свою очередь, направляет заявление о регистрации БПСА Оператору.

5.2.11.6. Оператор на основании заявления Участника осуществляет регистрацию БПСА в ПО Системы с присвоением соответствующих идентификаторов.

5.3. Критерии деятельности Участников в Системе

5.3.1. При осуществлении своей деятельности в рамках Системы Участники обязаны соблюдать следующие требования и обеспечить их соблюдение своими сотрудниками:

- соблюдать законодательства стран, вовлеченных в операцию по переводу денежных средств;
- отказать в проведении любой операции, относительно которой имеются подозрения в причастности к противоправным действиям;
- фиксировать сведения о Клиенте в требуемом объеме;
- направлять в уполномоченный государственный орган отчеты при выявлении операций, связанных с легализацией (отмыванием) доходов, полученных преступным путем, и финансированием террористической деятельности (если указанное требование предусмотрено законодательством, регулирующим деятельность Участника);
- не регистрировать заведомо ложные данные Клиента;
- не разглашать информацию о Клиентах и их операциях в Системе;
- не использовать информацию о Клиентах в иных целях;
- не информировать Клиентов и иных лиц о принимаемых мерах в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (если указанное требование предусмотрено законодательством, регулирующим деятельность Участника);
- хранить информацию о Клиентах и операциях в соответствии со стандартами безопасности не менее 5 лет со дня проведения операции Клиентом или со дня прекращения отношений с Клиентом;
- предоставлять доступ к работе с ПО Системы, используемого для обеспечения приема, передачи, хранения и обработки информации о переводах денежных средств, проводимых в связи с осуществлением переводов денежных средств, только сотрудникам, прошедшим обучение в сфере противодействия легализации денежных средств, полученных преступным путем, и финансирования терроризма, и ознакомленным с Правилами Системы;
- реализовывать мероприятия по противодействию осуществлению переводов денежных средств без добровольного согласия клиента.

5.4. Критерии приостановления и прекращения участия в Системе

5.4.1. **Приостановление участия в Системе**

5.4.1.1. Приостановление участия в Системе подразумевает блокирование Операционным центром по заявлению Участника или по решению Оператора возможности осуществления Участником всех или отдельных видов операций в Системе.

5.4.1.2. Приостановление участия в Системе является временным статусом Участника и предусматривает возможность восстановления Участником своего полного участия в Системе после ликвидации причин, приведших к необходимости приостановления участия.

5.4.1.3. Критерии приостановления участия в Системе:

- по инициативе Участника, на основании его письменного заявления в адрес Оператора, в случае если Участник по техническим или организационным причинам временно не может осуществлять свою деятельность в соответствии с настоящими Правилами. Восстановление полного участия в Системе осуществляется на основании письменного заявления Участника в адрес Оператора о возобновлении своего полного участия Платежной Системе. При получении заявления о приостановлении участия от Косвенного участника Оператор доводит указанную информацию до сведения Прямого участника по Согласованным каналам связи;

– по инициативе Оператора в случае нарушения настоящих Правил.

5.4.1.4. В случае принятия решения о временной приостановке деятельности Участника в Системе по инициативе Оператора, Оператор незамедлительно уведомляет Участника по Согласованным каналам связи о причинах приостановления участия и о необходимости устранения Участником допущенных нарушений в течение 30 (Тридцати) календарных дней.

5.4.1.5. После устранения Участником допущенных нарушений и их последствий, а также предоставления документов, подтверждающих их устранение, Оператор возобновляет деятельность Участника в Системе.

5.4.2. **Прекращение участия в Системе**

5.4.2.1. Прекращение участия в Системе подразумевает полное прекращение осуществления своих прав и обязанностей Участником в рамках Системы и расторжение Договора участия.

5.4.2.2. Критерии прекращения участия в Системе:

– По инициативе Участника. Участник уведомляет Оператора о прекращении своей деятельности в качестве Участника Системы и расторжении Договора участия не менее чем за 30 (Тридцать) календарных дней до предполагаемой даты прекращения участия в Системе. При получении заявления о прекращении участия от Косвенного участника Оператор доводит указанную информацию до сведения Прямого участника по Согласованным каналам связи.

– По инициативе Оператора в следующих случаях:

а) отзыва у Участника лицензии, в соответствии с которой Участник осуществляет деятельность по переводу денежных средств в соответствии с законодательством Российской Федерации или страны инкорпорации Участника;

б) в случае возбуждения процедуры банкротства в отношении Участника;

в) неосуществления Участником всех необходимых мер в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма;

г) нарушения Участником настоящих Правил при условии, что Участник не устранил такие нарушения в течение 30 (Тридцати) календарных дней после получения письменного уведомления о таком нарушении от Оператора и/или уведомления о приостановления участия;

д) наложения ареста на денежные средства на банковском Счете Участника, открытого в Расчетном центре Системы (у Прямого участника, в случае его открытия);

е) действия Участника представляют обоснованный риск для функционирования Системы.

5.4.2.3. В случае принятия решения о прекращении участия в Системе Оператор не позднее следующего рабочего дня после принятия решения, уведомляет Участника в письменном виде.

5.4.2.4. Участник Системы обязан не позднее 1 (Одного) рабочего дня, со дня получения уведомления от Оператора обеспечить осуществление расчетов по всем своим обязательствам.

5.5. Порядок привлечения Операторов услуг платежной инфраструктуры

5.5.1. В Системе возможно участие нескольких Операционных центров, Платежных клиринговых центров (в том числе выполняющих функции ЦПКК) и Расчетных центров.

5.5.2. Привлечение Операторов УПИ осуществляется на основании договоров с Оператором.

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

5.5.4. Для осуществления перевода денежных средств Участниками, находящимися на территории Российской Федерации, Оператор привлекает Операторов УПИ, которые находятся на территории Российской Федерации.

5.5.5. Оператор вправе привлекать Операционный центр, соответствующий требованиям законодательства Российской Федерации о национальной платежной системе.

5.5.6. Оператор УПИ осуществляет свою деятельность в соответствии с Правилами Платежной системы и договорами, заключаемыми с Оператором.

5.5.7. Операторы УПИ обязаны предоставлять Оператору информацию о своей деятельности (в части оказания услуг платежной инфраструктуры) в соответствии с Правилами.

5.5.8. Для участия в Платежной системе Оператор УПИ представляет подписанное со своей стороны соглашение о неразглашении конфиденциальной информации, заявление о Согласованных каналах связи и уполномоченных лицах по формам, предусмотренным Оператором, проект договора об оказании услуг платежной инфраструктуры, а также комплект документов, определенный Оператором.

5.5.9. Оператор осуществляет проверку Оператора УПИ на соответствие требованиям, установленным Правилами.

5.5.10. Оператор вправе запросить у Оператора УПИ дополнительные документы для проведения проверки.

5.5.11. В случае принятия положительного решения по результатам проверки на соответствие требованиям, установленным Правилами, Оператор заключает с Оператором УПИ договор на оказание соответствующих услуг в рамках Системы.

5.5.12. После заключения указанного договора, Оператор УПИ проводит все необходимые организационные и технологические процедуры для осуществления своей деятельности в Системе, включая проведение тестирования процедур и регламентов на соответствие требованиям Правил.

5.5.13. Оператор вносит информацию об Операторе УПИ в перечень Операторов УПИ.

5.5.14. Оператор ведет перечень Операторов УПИ и направляет его в Центральный банк Российской Федерации вместе с регистрационным заявлением на регистрацию в качестве Оператора Платежной системы в порядке и форме, установленном Банком России.

5.5.15. В случае привлечения новых Операторов УПИ или расторжения существующих договоров, Оператор направляет обновленный перечень Операторов УПИ в Центральный банк Российской Федерации в течение 10 (Десяти) дней с момента изменения перечня.

5.5.16. Перечень Операторов УПИ доводится до сведения Участников в ЛК или направляется по Согласованным каналам связи.

5.5.17. К Операционным центрам и Платежным клиринговым центрам предъявляются следующие требования:

- устойчивое финансовое состояние: платежеспособность, не зависящая от кредитования, отсутствие задолженности по оплате в бюджет Российской Федерации и другие показатели финансовой устойчивости. Оценка финансового состояния осуществляется на основании бухгалтерского баланса и иных документов, характеризующих финансовое состояние Операционного центра и/или Платежного клирингового центра;
- использование оборудования и программного обеспечения, которые обеспечивают сохранение банковской тайны, защиту информации и персональных данных в соответствии с законодательством Российской Федерации, резервирования оборудования и каналов передачи информации и другие требования, выполнение которых необходимо для обеспечения БФПС (раздел 9 настоящих Правил);
- обеспечение конфиденциальности информации об операциях и о Счетах Участников и их Клиентов, полученные при оказании операционных услуг и/или услуг платежного клиринга,

за исключением передачи информации в рамках Платежной системы, а также случаев, предусмотренных федеральными законами;

- реализация мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента.

5.5.18. К Расчетным центрам, в том числе совмещающим свою деятельность с деятельностью ПКЦ, выполняющего функции ЦПКК, предъявляются следующие требования:

- Расчетным центром должна выступать только кредитная организация;
- кредитная организация должна иметь технологическую возможность подключения к ПО Системы;
- кредитная организация должна соответствовать категории финансово стабильных кредитных организаций и требованиям по управлению рисками, установленными Банком России;
- кредитная организация, привлекаемая в качестве Расчетного центра, обеспечивает банковскую тайну, защиту информации о средствах и методах обеспечения информационной безопасности и персональных данных клиентов в соответствии с законодательством Российской Федерации;
- кредитная организация выполняет требования законодательства Российской Федерации по противодействию легализации (отмыванию) доходов, полученных преступным путем и финансированию терроризма;
- кредитная организация реализует мероприятия по противодействию осуществлению переводов денежных средств без добровольного согласия клиента.

6. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ

6.1. Применяемые формы безналичных расчетов

6.1.1. Перевод денежных средств осуществляется со Счета Участника на основании распоряжений Отправителя или требований Получателя, включенных в платежную клиринговую позицию Участника, и в Реестр, поступающий в Расчетный центр от Платежного клирингового центра Системы по каналам связи, определенным в договоре между Расчетным центром и Оператором Системы, выступающим в качестве Операционного центра и Платежного клирингового центра.

6.1.2. В целях осуществления Переводов на территории Российской Федерации в Системе применяются следующие формы безналичных расчетов при переводе денежных средств в соответствии с Положением Банка России от 29 июня 2021 №762-П «О правилах осуществления перевода денежных средств»:

- расчеты платежными поручениями;
- расчеты в форме перевода денежных средств по требованию получателя средств (прямое дебетование).

В рамках Системы могут осуществляться безналичные расчеты в форме перевода Электронных денежных средств, а также в Системе осуществляются операции перевода остатка (его части) Электронных денежных средств и операции перевода с целью увеличения остатка Электронных денежных средств в соответствии с требованиями законодательства Российской Федерации.

Учет информации об остатках Электронных денежных средств осуществляют Участники Системы, являющиеся одновременно Операторами электронных денежных средств.

6.1.3. Трансграничные Переводы по Системе осуществляются в соответствии с законодательством Российской Федерации/страны инкорпорации Участника, настоящими Правилами, соглашениями с иностранными участниками и Партнерами с учетом международной банковской практики.

6.2. Совершаемые операции

6.2.1. Предоставление и использование Услуг Системы реализуется выполнением операций. Системой предусмотрены следующие виды операций:

- прием, оформление и отправка новых Переводов.
- оформление, формирование и отправка запроса на изменение реквизитов ранее отправленного Перевода.
- оформление, формирование и отправка запроса на возврат Перевода.
- получение, оформление и выдача (зачисление) поступивших и возвращенных Переводов.

6.2.2. Осуществление операций производится с использованием ПО Системы.

6.2.3. Состав и формат информации, необходимой для осуществления операций, определяется Оператором Системы, содержится в Системе и контролируется ПО Системы.

6.2.4. Реквизиты Получателей – юридических лиц/индивидуальных предпринимателей содержатся в ПО Системы, либо вводятся в момент оформления операции, в том числе из информационных систем Участника.

6.3. Порядок осуществления перевода денежных средств (приема, оформления и отправки новых Переводов), в т.ч. моменты наступления его безотзывности, безусловности и окончательности перевода

6.3.1. Прием, оформление и отправка новых Переводов осуществляется Участником-отправителем за счет денежных средств, предоставленных Отправителем. Участник-отправитель отказывает Отправителю в приеме его денежных средств или Распоряжения к исполнению при недостаточности

предоставленных денежных средств для осуществления Перевода с учетом комиссии, подлежащей уплате Отправителем.

6.3.2. В случаях, предусмотренных законодательством страны местонахождения Участника-отправителя, а также в случаях наличия требований Системы, приём от Отправителя – физического лица денежных средств для осуществления Перевода производится с обеспечением процессов идентификации (аутентификации) Отправителя.

6.3.3. Под идентификацией понимается комплекс мер по установлению сведений о физическом лице, по подтверждению достоверности этих сведений.

6.3.4. Под аутентификацией понимается комплекс мер по проверке подлинности и принадлежности идентификационных данных физическому лицу.

6.3.5. Идентификация осуществляется на основании документа, удостоверяющего личность, содержащего сведения, достаточные для проведения идентификации физического лица и осуществления операции. На основании указанного документа данные вносятся в программное обеспечение Системы. Идентификация также может осуществляться иными способами в соответствии с законодательством страны местонахождения Участника.

6.3.6. Участник в соответствии с действующим законодательством страны своего местонахождения имеет право запросить у физического лица иные документы, необходимые для его идентификации.

6.3.7. Аутентификация используется в случае применения средств ДБО.

6.3.8. Аутентификация производится следующими способами:

– средствами аутентификации, определяемыми Участником-отправителем самостоятельно, при условии обеспечения передачи данных об Отправителе в объеме, достаточном для соблюдения требований законодательства и Системы;

– средствами аутентификации, определяемыми Участником-отправителем и Оператором Системы путем заключения дополнительных договоров.

6.3.9. При отправке Перевода Оператором Системы присваивается уникальный идентификатор (контрольный номер перевода и(или) идентификатор операции в Системе).

6.3.10. Участник-отправитель предоставляет Отправителю документ, подтверждающий осуществление операции, и сведения об операции в электронном виде или на бумажном носителе. В случае отправки документа в электронном виде, Отправитель должен иметь возможность получения копии документа на бумажном носителе. Участник-отправитель в случае применения средств ДБО имеет право направлять подтверждение о совершении операции и сведения о ней только в электронном виде.

6.3.11. Документ, подтверждающий факт осуществления операции, обязательно должен содержать следующую информацию:

- указание, что операция совершена по Системе;
- номер операции (уникальный идентификатор);
- дату операции;
- место совершения операции;
- сумму и валюту совершения операции, комиссию за совершение операции (при наличии);
- фамилию, имя и отчество (при его наличии) Отправителя – физического лица (по Переводам, осуществляемым с идентификацией Отправителя);
- реквизиты Участника, куда Отправитель может обратиться в случае возникновения претензий;

– обменный курс при отличии валюты переводимых денежных средств и валюты, в которой осуществляется выплата, либо сумма в валюте отправления и сумма в валюте получения денежных средств (при необходимости).

В дополнение к указанным выше реквизитам в документе, подтверждающем осуществление операции, должны содержаться следующие сведения:

а) при направлении средств в адрес физических лиц для выдачи наличных:

– страна и город назначения Перевода (при наличии);

– место выдачи (при наличии);

– фамилия, имя и отчество (при его наличии) Получателя-физического лица;

– дополнительная информация, необходимая для идентификации Отправителя и/или Получателя, необходимая Участнику-получателю для совершения выплаты Перевода (при наличии соответствующих требований со стороны Участника-получателя, в том числе в соответствии с требованиями применимого законодательства).

б) при направлении средств в адрес физических лиц для зачисления на карту/счет или для увеличения остатка ЭДС:

– страна и город назначения Перевода (при наличии);

– дополнительная информация, необходимая для идентификации Отправителя и/или Получателя, необходимая Участнику-получателю для зачисления Перевода (при наличии соответствующих требований со стороны Участника-получателя, в том числе в соответствии с требованиями применимого законодательства (например, номер карты, и(или) номер телефона, и(или) номер счета, и(или) фамилия, имя и отчество (при его наличии) Получателя-физического лица, и(или) дата рождения и(или) иные сведения)).

в) при направлении средств в адрес юридических лиц/индивидуальных предпринимателей[1]:

– наименование Получателя;

– идентификатор в системе Получателя (номер договора, номер телефона, номер клиента и т.д.);

– реквизиты Получателя, если они вводятся в момент оформления операции.

6.3.12. Информация об Отправителе и Получателе передается по всей цепочке прохождения операции.

6.3.13. При направлении средств в адрес физических лиц с целью выдачи наличных денежных средств Участник-отправитель доводит до сведения Отправителя информацию о том, что:

– для получения наличных денежных средств Отправитель обязан самостоятельно сообщить исключительно Получателю о факте отправки денежных средств, что операция проведена по Системе и (или) рамках иной платежной системы, с которой Оператор Системы установил межсистемное взаимодействие (если условиями выдачи Перевода, установленными выбранным Участником-получателем, не обусловлено указание Получателем иной идентифицирующей информации), а также информацию, необходимую Получателю для выплаты Перевода, в т.ч. уникальный идентификатор, сумму и валюту Перевода, адрес(а) пункта(ов) получения (при необходимости) (далее – иные реквизиты);

– недопустимо сообщать уникальный идентификатор (контрольный номер перевода и(или) идентификатор операции в Системе), а также иные реквизиты Перевода, включая данные Получателя, третьим лицам.

[1] Здесь и далее: операция в пользу Получателя-юридического лица/индивидуального предпринимателя осуществляется в случае отсутствия ограничений, предусмотренных законодательством страны инкорпорации Участника.

В зависимости от технологии выдачи Перевода (адресная или безадресная) Получатель должен будет обратиться в выбранный Отправителем пункт (адресная технология выдачи), или в любой пункт Системы или иной платежной системы, с которой Оператор Системы установил межсистемное взаимодействие, в выбранном Отправителем городе или стране (безадресная технология выдачи). При этом Оператор Системы предоставляет возможность выдачи Безадресного перевода в любом пункте выбранной Отправителем страны, а указание Отправителем определенного города получения в данном случае обусловлено необходимостью убедиться, что в интересующем Отправителя населенном пункте имеется хотя бы один пункт выдачи Переводов Системы, включая выдачу в пунктах иной платежной системы, с которой Оператор Системы установил межсистемное взаимодействие.

6.3.14. Перевод Электронных денежных средств осуществляется Участником, являющимся Оператором электронных денежных средств, на основании договора, заключенного с Клиентом-физическим лицом. Предоставление Клиентом-физическим лицом Оператору электронных денежных средств осуществляется в соответствии с требованиями Федерального закона №161-ФЗ.

6.3.15. Перевод Электронных денежных средств осуществляется путем одновременного принятия Оператором электронных денежных средств распоряжения Клиента-физического лица, уменьшения им остатка Электронных денежных средств Отправителя и увеличения им остатка Электронных денежных средств Получателя средств на сумму перевода Электронных денежных средств либо в случае осуществления перевода Электронных денежных средств с использованием предоплаченной карты в срок не более 3 (трех) рабочих дней после принятия Оператором электронных денежных средств распоряжения Клиента-физического лица, если более короткий срок не предусмотрен договором Участника с Клиентом-физическим лицом.

6.3.16. Автономный режим использования Электронного средства платежа в Системе не предусматривается.

6.3.17. Порядок использования Электронных средств платежа при осуществлении переводов Электронных денежных средств регулируется условиями договоров Участников Платежной системы и их Клиентов. Участники-резиденты Российской Федерации гарантируют осуществление перевода Электронных денежных средств в соответствии со статьей 7 Федерального закона №161-ФЗ с учетом особенностей перевода Электронных денежных средств с использованием Электронных средств платежа, предусмотренных статьей 10 Федерального закона №161-ФЗ.

6.3.18. В случае осуществления Участниками – Операторами электронных денежных средств в рамках Платежной системы перевода Электронных денежных средств, порядок таких переводов должен соответствовать следующим требованиям:

6.3.18.1. Перевод Электронных денежных средств осуществляется Участником, являющимся Оператором электронных денежных средств, с проведением идентификации Клиента, упрощенной идентификации Клиента – физического лица или без проведения идентификации в соответствии с Федеральным законом от 07.08.2001 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» (далее – «Федеральный закон №115-ФЗ»).

6.3.18.2. В случае проведения Оператором электронных денежных средств идентификации Клиента – физического лица в соответствии с Федеральным законом №115-ФЗ использование Электронного средства платежа осуществляется Клиентом - физическим лицом при условии, что остаток Электронных денежных средств в любой момент не превышает 600 000 (шестьсот тысяч) рублей либо сумму в иностранной валюте, эквивалентную 600 000 (шестистам тысячам) рублей по официальному курсу Банка России. Указанное Электронное средство платежа является персонифицированным. Допускается превышение суммы, указанной в настоящем пункте, вследствие изменения официального курса иностранной валюты, устанавливаемого Банком России.

6.3.18.3. В случае непроведения Оператором электронных денежных средств идентификации Клиента - физического лица в соответствии с Федеральным законом №115-ФЗ использование Электронного средства платежа осуществляется Клиентом - физическим лицом при условии, что остаток Электронных денежных средств в любой момент не превышает 15 000 (пятнадцать тысяч)

рублей, за исключением случая, предусмотренного п. 6.3.18.5 Правил. Указанное электронное средство платежа является неперсонифицированным.

6.3.18.4. Общая сумма переводимых Электронных денежных средств с использованием одного неперсонифицированного Электронного средства платежа не может превышать 40 000 (сорок тысяч) рублей в течение календарного месяца, за исключением случая, предусмотренного п. 6.3.18.5 Правил.

6.3.18.5. В случае проведения Участником – Оператором электронных денежных средств упрощенной идентификации Клиента - физического лица в соответствии с Федеральным законом №115-ФЗ использование неперсонифицированного Электронного средства платежа может осуществляться Клиентом – физическим лицом при условии, что остаток Электронных денежных средств в любой момент не превышает 100 000 (сто тысяч) рублей, а общая сумма переводимых Электронных денежных средств с использованием такого неперсонифицированного Электронного средства платежа не превышает 200 000 (двести тысяч) рублей в течение календарного месяца.

6.3.18.6. Неперсонифицированное Электронное средство платежа не может использоваться Клиентом - физическим лицом, не прошедшим упрощенную идентификацию, для осуществления перевода Электронных денежных средств другому физическому лицу либо для получения переводимых Электронных денежных средств от другого физического лица.

6.3.18.7. Участник – Оператор электронных денежных средств не осуществляет перевод Электронных денежных средств, если в результате такого перевода будут превышены суммы, указанные в п. 6.3.18.2 - 6.3.18.5 Правил. При этом за счет остатка (его части) Электронных денежных средств:

– Клиента - физического лица, использующего персонифицированное Электронное средство платежа, денежные средства могут быть по его распоряжению переведены на банковский счет, направлены на исполнение обязательств Клиента - физического лица перед кредитной организацией, филиалом иностранного банка, переведены без открытия банковского счета или выданы наличными денежными средствами;

– Клиента - физического лица, использующего неперсонифицированное Электронное средство платежа, денежные средства могут быть по его распоряжению переведены на банковский счет в пользу юридических лиц, индивидуальных предпринимателей, направлены на исполнение обязательств Клиента – физического лица перед кредитной организацией, филиалом иностранного банка, а также, если указанный Клиент прошел процедуру упрощенной идентификации, переведены на банковские счета физических лиц или выданы ему наличными денежными средствами в случае использования предоплаченной карты при условии, что общая сумма выдаваемых наличных денежных средств не превышает 5 000 (пять тысяч) рублей в течение одного календарного дня и 40 000 (сорок тысяч) рублей в течение одного календарного месяца.

6.3.19. По Переводам в пользу физических лиц для выплаты наличными денежными средствами безусловность Перевода наступает в момент обращения Получателя в точку выплаты при выполнении следующих условий: совпадении информации об уникальном идентификаторе операции, содержащемся в Системе, с уникальным идентификатором, указанным Получателем, совпадении данных о Получателе, переданными по цепочке прохождения операции, с данными в предъявленном документе, удостоверяющем личность.

6.3.20. По Переводам в пользу юридических лиц и индивидуальных предпринимателей, или для зачисления на счета/карты, или для увеличения остатка ЭДС Клиентов-физических лиц, в том числе с целью погашения кредита, при наличии у Участника-получателя или самого Получателя индивидуальных требований к информации, которая должна содержаться в Переводе в их пользу, безусловность наступает в момент введения информации о Переводе в используемое Участником-отправителем программное обеспечение и получения программным способом ответа от Оператора о присвоении Переводу статуса, подтверждающего его прием к исполнению. Проверка наступления безусловности может осуществляться:

- на этапе введения Перевода в программное обеспечение Участника-отправителя (при использовании Участником ПО Системы, поставляемого Оператором Системы, такая проверка осуществляется автоматически), при непрохождении проверки Перевод не принимается в обработку;
- на этапе обработки Перевода Платежным клиринговым центром, в этом случае при непрохождении проверки Перевод возвращается Участнику-отправителю Платежным клиринговым центром;
- самим Участником-получателем или Получателем - юридическим лицом/индивидуальным предпринимателем при поступлении информации о Переводе.

6.3.21. Безотзывность Переводов, направленных Отправителями как для выдачи наличными, так и для зачисления в пользу юридических лиц и индивидуальных предпринимателей, или для зачисления на счета/карты, увеличения остатка ЭДС, в том числе с целью погашения кредита, 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-получателем, или с иной платежной системой, с которой Оператор Системы установил межсистемное взаимодействие, или не обусловлено применяемой формой безналичных расчетов.

6.3.22. Окончательность Перевода, направленного Отправителем как для выдачи наличными, так и для зачисления в пользу юридических лиц и индивидуальных предпринимателей, или для зачисления на счета/карты, увеличения остатка ЭДС, в том числе с целью погашения кредита, наступает в момент зачисления денежных средств на Счет Участника-получателя или иной платежной системы, с которой Оператор Системы установил межсистемное взаимодействие с учетом порядка и условий осуществления клиринга и расчетов, осуществляемых в Системе.

6.3.23. Перевод Электронных денежных средств становится безотзывным и окончательным после осуществления Оператором электронных денежных средств действий, указанных в п. 6.3.15 Правил.

6.3.24. Оператор Системы в течение 24 часов с момента принятия Перевода от Участника-отправителя к исполнению обеспечивает доступность Перевода к выплате/зачислению Получателю у Участника-получателя в стране, в которой находится выбранный Отправителем город (при безадресной технологии), либо доступность информации о Переводе Участнику-получателя (при адресной технологии).

6.3.25. Оператор Системы обеспечивает доступность информации о принятом к исполнению Переводе Клиенту – юридическому лицу/индивидуальному предпринимателю, либо кредитной организации, в которой открыт счет Получателя в сроки, определяемые условиями информационного обмена, содержащимися в соответствующих договорах с ними.

6.3.26. После приема наличных денежных средств от Отправителя, или списания со счета Отправителя, или уменьшения остатка ЭДС и получения от Платежного клирингового центра подтверждения прохождения Переводом проверки на соответствие всем необходимым требованиям, ответственные сотрудники Участника-отправителя обязаны незамедлительно закончить процедуру оформления Перевода в соответствии с требованиями используемого ПО Системы для скорейшей отправки Перевода в Платежный клиринговый центр.

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

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

6.4.2. Внесение изменений в Перевод, направленный в пользу физического лица для выплаты наличными денежными средствами, возможно осуществить по требованию Отправителя при условии, что на момент внесения изменений или передачи их в Операционный центр денежные средства не

были выплачены Получателю. Внесение изменений возможно только в реквизиты Получателя – физического лица (фамилия, имя, отчество (при наличии)) или дополнительную информацию.

6.4.3. Для внесения изменений в Перевод, направленный для зачисления на карту/счет, или для увеличения остатка ЭДС Клиента-физического лица, или в пользу Клиента-юридического лица/индивидуального предпринимателя, Отправитель обращается к соответствующему Получателю - юридическому лицу/индивидуальному предпринимателю или к кредитной организации/иностранному банку, в котором открыт счет Получателя, напрямую. В случае невозможности такого обращения Отправитель может подать Участнику-отправителя соответствующее заявление. При этом сама возможность внесения изменений в такой Перевод по Системе, а также порядок и сроки внесения изменений, определяются условиями информационно-технологического взаимодействия с контрагентом, обеспечивающим зачисление денежных средств Получателю.

6.4.4. Условием осуществления операции является предъявление Отправителем документа, подтверждающего факт совершения отправки, и, при необходимости, документов, подтверждающих, что он является Отправителем.

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

6.4.6. Участник-отправителя, принявший заявление Отправителя на внесение изменений, обязан незамедлительно с момента его принятия направить запрос на изменение Оператору Системы. В случае невозможности внесения изменений в Перевод по причине его выдачи или в соответствии с условиями осуществления Перевода, установленными Участником-получателем, передача такого запроса программным способом Оператором Системы невозможна.

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

6.4.8. Дополнительная комиссия за внесение изменений не взимается, если иное не оговорено в договорах с соответствующими юридическими лицами/индивидуальными предпринимателями – Получателями, кредитными организациями, в которых открыты счета/карты или осуществляется учет ЭДС Получателей.

6.5. Порядок оформления, формирования и отправки запросов на возврат Переводов

6.5.1. Порядок возврата денежных средств при совершении операции Участником-отправителя с использованием средств ДБО, со счетов Отправителя определяется и доводится до сведения Отправителя Участником-отправителем самостоятельно с учетом требований, предусмотренных Правилами.

6.5.2. Возврат Перевода осуществляется только по запросу Отправителя, если иное не установлено соглашением между Оператором Системы и Участником-отправителем или Участником-получателем (в том числе являющемся участником или расчетным центром платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие), в том числе при совершении операции с использованием ДБО.

6.5.3. При возврате Безадресного перевода комиссия, уплаченная Отправителем, подлежит возмещению при условии, что Перевод не осуществлен по причинам на стороне (по вине) Участника-отправителя[1] и запрос на возврат сформирован Участником-отправителем данного Безадресного перевода, т.е. офисом Участника, из которого был первоначально отправлен Перевод, или в любых других офисах этого же Участника-отправителя. В этом случае комиссия Отправителю возвращается Участником-отправителем в той же сумме и валюте, в которой она была удержана с него при отправке такого Перевода, одновременно с суммой Перевода. Допускаются исключения, когда из-за

[1] К Переводам, совершенным Участником, относятся также Переводы, совершенные привлеченными им Партнерами и(или) БПА (БПСА).

технологических особенностей способа осуществления Перевода у некоторых Участников (отправка с помощью определенных средств ДБО) комиссия по вышеупомянутым Переводам возврату не подлежит, о чем указанные Участники обязаны извещать Отправителей-физических лиц доступным способом до совершения операции. По прочим Переводам, в том числе в случае возврата Перевода по инициативе Отправителя (в случае допущенных Отправителем ошибок в Переводе и т.п.), комиссия, уплаченная Отправителем, при возврате денежных средств Отправителю не возмещается (если иное не предусмотрено договорами Оператора Системы с Участником-получателем и(или) оператором иной платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие).

Если за осуществление Перевода комиссию Участнику-отправителю уплачивал Оператор Системы, то возврат такого Перевода осуществляется при условии возмещения Участником-отправителем Оператору Системы ранее уплаченной комиссии. Участник-отправителя вправе в дальнейшем взыскать сумму возмещенной Оператору Системы комиссии с Отправителя.

6.5.4. Оператор Системы предоставляет физическим лицам - Отправителям возможность запросить отправляемые ими Безадресные переводы на возврат в офисах участников платежной системы, с которой Оператор Системы установил межсистемное взаимодействие, если такая возможность установлена правилами данной платежной системы и(или) договором Оператора Системы с оператором иной платежной системы.

6.5.5. В случае невозможности оформления Отправителем Безадресного перевода на возврат в офисах Участника-отправителя, Отправитель, руководствуясь положениями п. 6.4. Правил, может направить Участнику-отправителю запрос на изменение реквизитов ранее отправленного Перевода, изменив данные Получателя на данные Отправителя, и получить данный Перевод, как Получатель Перевода (возврат через выдачу) в офисах других Участников Системы в стране получения Перевода или в офисах участников платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие, согласно правилам данной платежной системы (если Перевод был отправлен в рамках межсистемного взаимодействия Оператора с другой платежной системой).

6.5.6. Возврат Перевода, направленного в пользу физического лица для выплаты наличными денежными средствами, может быть осуществлен только в случае, если на момент запроса или передачи его в Операционный центр денежные средства еще не выплачены Получателю. В противном случае Участник самостоятельно несет риски, в том числе финансовые, связанные с возвратом денежных средств Отправителю до момента получения подтверждения от Оператора о возможности его возврата. В случае возврата Перевода Отправителю до получения подтверждения от Оператора Системы Участник не вправе требовать от Оператора возврата указанного Перевода и обязан полностью осуществить расчет с Субъектами Системы по осуществленной, но впоследствии возвращенной, операции.

6.5.7. Для возврата денежных средств, направленных для зачисления на счета/карты, или для увеличения остатка ЭДС Клиентов-физических лиц, или направленных в пользу юридических лиц/индивидуальных предпринимателей, Отправитель обращается к соответствующему Получателю - юридическому лицу/индивидуальному предпринимателю или к кредитной организации/иностранному банку, в котором открыт счет/карта или осуществляется учет ЭДС Получателя, напрямую. В случае невозможности такого обращения Отправитель может подать в офис Участника-отправителя соответствующее заявление. При этом сама возможность возврата такого Перевода по Системе, а также его порядок и сроки, определяются условиями информационно-технологического взаимодействия с контрагентом, обеспечивающим зачисление денежных средств Получателю.

6.5.8. По исполненным трансграничным Переводам, направленным для зачисления на счет/карту или для увеличения остатка ЭДС Получателя, могут применяться особые условия возврата Перевода: за вычетом комиссии и/или расходов организации, в которой открыт счет/карта или осуществляется учет ЭДС Получателя. Информация о наличии таких условий содержится в особенностях осуществления Переводов, которые размещены на официальном сайте Системы или на сайте иной платежной системы, с которой Оператор Системы установил межсистемное взаимодействие, и предоставляются Участникам посредством ПО Системы в момент осуществления Перевода.

6.5.9. Условием осуществления операции возврата через Систему является предъявление Отправителем документа, подтверждающего факт совершения отправки, и, при необходимости, документов, подтверждающих, что он является Отправителем и (или) Получателем.

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

6.5.11. Участник-отправителя, принявший заявление Отправителя на возврат денежных средств, обязан незамедлительно с момента его принятия направить запрос на возврат Оператору Системы. В случае невозможности возврата Перевода по причине его выдачи или в соответствии с условиями осуществления Перевода, установленными Участником-получателем, передача такого запроса программным способом Оператором Системы невозможна.

6.5.12. Участник-отправителя уведомляет Отправителя о результатах обработки запроса.

6.5.13. В случае ошибочного совершения операции отправки по вине Участника-отправителя запрос на возврат инициируется Участником-отправителя. В этом случае, если комиссия не подлежит возврату, то она может быть возвращена по результатам расследования, проводимого Оператором Системы на основании письменного заявления Участника-отправителя, направляемого Оператору Системы.

6.5.14. В случае возврата Безадресного перевода по инициативе Отправителя или Участника-отправителя Оператором Системы вместе с суммой Безадресного перевода осуществляется возврат Участнику-отправителю комиссии, ранее уплаченной им Оператору Системы при отправке такого Перевода, при условии, что запрос на возврат для выдачи аннулированного Перевода Отправителю сформирован Участником-отправителем данного Безадресного перевода. При возврате через выдачу Участнику, выдавшему Перевод, программно-сформированный в пользу Отправителя, уплачивается комиссия, причитающаяся ему в соответствии с Тарифами Системы как Участнику-получателю аналогичного Перевода, направляемого от Участника-отправителя аннулированного Перевода.

6.5.15. В случае ошибочного направления Перевода в пользу физического лица для выплаты наличными денежными средствами в стране, Участники которой осуществляют такие выплаты по безадресной технологии, по вине Участника-отправителя и направления от его имени запроса на аннулирование ошибочной операции в течение одного операционного дня и при отсутствии каких-либо расчетов с Участником Получателя возможно осуществление данных операций без отражения в расчетах при условии уведомления Оператора Системы до проведения расчетов по итогам Операционного дня с Участником-отправителем.

Уведомление Оператора возможно осуществить любым доступным способом:

- по Согласованным каналам связи;
- по электронной почте службы технической поддержки Оператора, указанной на официальном сайте Оператора в сети Интернет.

6.5.16. В случае, если Перевод подлежит выдаче/зачислению Получателю в иной платежной системе, с которой Оператор Системы установил межсистемное взаимодействие, или Участником-получателем, или контрагентами Участника-получателя, у которого(ых) после осуществления Перевода Отправителем отозвана лицензия на осуществление банковских операций или иное разрешение на оказание услуг по переводу денежных средств по банковским счетам и (или) без открытия банковских счетов и (или) осуществление операций с использованием Электронных средств платежа, при условии, что денежные средства Отправителя по такому Переводу зачислены Расчетным центром (в том числе предварительно) на счета иной платежной системы и(или) Участнику-получателя, возврат такого перевода не осуществляется. Для возврата такого Перевода Клиенту необходимо предъявлять требования к временной администрации (ликвидатору, конкурсному управляющему) о включении своих требований в реестр требований кредиторов в порядке, предусмотренном действующим законодательством.

6.5.17. Возврат Бивалютного перевода осуществляется Участником-отправителем в валюте отправки.

6.6. Порядок возврата Переводов, отвергнутых Получателем-юридическим лицом или кредитной организацией

6.6.1. Возврат ранее исполненного Распоряжения может быть осуществлен по инициативе Получателя - юридического лица/индивидуального предпринимателя или кредитной организации в случае, если информация, необходимая для успешного зачисления денежных средств, указана некорректно или по иным причинам, возникшим на стороне Получателя - юридического лица/ индивидуального предпринимателя или кредитной организации.

6.6.2. В этом случае Отправителю должны быть возвращены денежные средства по операции. При этом комиссия, уплаченная Отправителем, при возврате денежных средств ему не возмещается. Если за осуществление Перевода комиссию Участнику-отправителю уплачивал Оператор Системы, то возврат такого Перевода осуществляется при условии возмещения Оператору Системы ранее уплаченной комиссии, если иное не оговорено в соглашениях, заключенных с соответствующими Получателями. Участник-отправитель вправе в дальнейшем взыскать сумму возмещенной Оператору Системы комиссии с Отправителя.

6.6.3. При возврате исполненного трансграничного Перевода по инициативе Получателя согласно п. 6.6.1. Правил, из суммы возвращаемых денежных средств могут быть удержаны комиссия и(или) иные расходы организации Получателя, связанные с возвратом трансграничного Перевода. Особые условия возврата предоставляются Участникам посредством программного обеспечения Оператора Системы, в момент осуществления Перевода.

6.6.4. Возврат денежных средств Отправителю осуществляется Участником-отправителем, который произвел первоначальное оформление и направление Распоряжения.

6.6.5. Возврат Бивалютного перевода осуществляется Участником-отправителем в валюте отправки.

6.7. Порядок получения, оформления и выдачи (зачисления) поступивших Переводов и Переводов к возврату

6.7.1. Выдача денежных средств осуществляется Участником-получателем путем выдачи Получателю наличных денежных средств без открытия счета (только для Получателей – физических лиц), путем зачисления на банковские счета Получателя (для Получателей-физических и юридических лиц/ индивидуальных предпринимателей), путем зачисления на банковские счета/карты физических лиц, путем увеличения остатка ЭДС.

6.7.2. Получатель обязан самостоятельно совершить действия, направленные на получение наличных денежных средств, в течение 90 (девяносто) календарных дней с даты отправки денежных средств Отправителем, если иной срок не установлен договором Оператора с Участником и(или) иными договорами. По истечении указанного срока Перевод недоступен для выдачи Получателю. Дальнейшее истребование денежных средств по такому Переводу возможно только по требованию Отправителя в течение 3 (трех) лет с момента готовности Перевода к выдаче Получателю (п. 6.3.24 Правил).

6.7.3. При выдаче наличных денежных средств без открытия счета Участник-получатель должен идентифицировать Получателя на основе документа, удостоверяющего личность, либо иным способом в соответствии с законодательством страны своего местонахождения. В случае обращения для получения денежных средств представителя Получателя с надлежащим образом оформленной доверенностью Участник-получатель получатель вправе отказать в выдаче денежных средств.

6.7.4. Участник в соответствии с действующим законодательством страны своего местонахождения имеет право запросить у физического лица иные документы, необходимые для его идентификации, а также осуществить процедуры аутентификации (при необходимости).

6.7.5. Выдача наличных денежных средств Получателю возможна при условии совпадения информации о номере операции (уникальный идентификатор) с номером, указанным Получателем,

данных о Получателе, переданными по цепочке прохождения операции, с данными в предъявленном документе, удостоверяющем личность, т.е. наступлении Безусловности перевода денежных средств.

6.7.6. Зачисление денежных средств осуществляется при совпадении реквизитов, указанных в Переводе, с реквизитами Получателя, имеющимися у Участника-получателя.

6.7.7. Не допускается отказ в выдаче наличных денежных средств в случае расхождений в написании данных Получателя-физического лица в полученной информации об операции и предъявленном документе в следующих случаях:

- 1-2 ошибки в написании данных, вызванные возможностью разновариантного, сокращенного написания или опечаткой;
- если в Переводе Ф.И.О. Получателя указано в дательном падеже;
- если поля «Фамилия Получателя», «Имя Получателя» и «Отчество Получателя» заполнены в некорректной последовательности, но при этом позволяют однозначно идентифицировать Клиента в соответствии с его документом, удостоверяющим личность;
- если документ, удостоверяющий личность, не предполагает указание отчества, но отчество указано в полученной информации об операции; в этом случае отчество используется в качестве дополнительного идентификатора;
- если документ, удостоверяющий личность, предполагает указание отчества, но отчество не указано в полученной информации об операции;
- если в полученной информации об операции фамилия, имя и отчество Получателя указано латинскими буквами, а в документе, удостоверяющем личность – русскими, и наоборот.

Выплата денежных средств, поступивших от юридических лиц/индивидуальных предпринимателей – Клиентов Участников и (или) Оператора Системы имеет особенности: запрещено вносить какие-либо изменения в данные Получателя, а также выплачивать денежные средства при наличии расхождений в данных Получателя в полученной информации об операции и в предъявленном Получателем документе, удостоверяющим личность. При необходимости внесения изменений в данные Получателя перевод денежных средств подлежит аннулированию Отправителем - юридическим лицом/индивидуальным предпринимателем.

6.7.8. Участник-получатель не несет ответственности за отказ в выплате денежных средств при несоответствии сведений, предоставленных Получателем, со сведениями, указанными при отправлении денежных средств Участником-отправителем и/или Отправителем.

6.7.9. При необходимости у Получателя могут быть запрошены дополнительные сведения об операции.

6.7.10. Выплата может производиться:

- в валюте, в которой направлены денежные средства,
- в иной валюте при осуществлении перевода денежных средств с различными валютами отправки и выплаты,
- в иной валюте по согласованию с Получателем – физическим лицом.

6.7.11. По согласованию с Оператором Системы в отдельных случаях или в соответствии с требованиями законодательства страны инкорпорации Участника выплата денежных средств некоторыми Участниками может осуществляться исключительно в национальной валюте страны Участника, либо исключительно путем зачисления денежных средств на счета/карты или увеличения остатка ЭДС Получателя, либо иным способом в соответствии с законодательством этих стран. Информация об этом доводится до сведения Участников в ПО Системы или по Согласованным каналам связи.

6.7.12. Участник-получатель предоставляет Получателю документ, подтверждающий осуществление операции, и сведения об операции в электронном виде или на бумажном носителе. В случае

предоставления документа в электронном виде Получатель должен иметь возможность получения документа на бумажном носителе.

6.7.13. Документ, подтверждающий факт осуществления операции, обязательно должен содержать следующую информацию:

- указание, что операция совершена по Системе (при наличии технической возможности);
- номер операции (уникальный идентификатор);
- дату операции;
- место совершения операции;
- сумму и валюту совершения операции;
- реквизиты Получателя.

6.7.14. Участник-получатель обязан незамедлительно в момент выплаты направить Оператору Системы подтверждение о выплате/зачислении.

6.7.15. При проставлении ошибочной отметки о выплате Перевода Участником-получателем последний обязан уведомить о данном факте Оператора Системы любым доступным способом:

- по Согласованным каналам связи;
- по электронной почте службы технической поддержки Оператора, указанной на официальном сайте Оператора в сети Интернет.

6.7.16. В случае, если уведомление, предусмотренное п. 6.7.15 Правил, получено и обработано Оператором Системы в день проставления ошибочной отметки о выплате Перевода, при этом перевод фактически не выплачен Получателю, Оператор Системы изменяет статус этого Перевода на успешный, при этом такая операция не подлежит отражению в Отчете Участника-получателя за этот операционный день.

В случае если уведомление получено Оператором по окончании операционного дня, в котором Участник-получатель допустил ошибку, и по данному Переводу были проведены расчеты, Участник-получатель самостоятельно предпринимает все необходимые действия для выдачи/зачисления этого Перевода Клиенту (Получателю).

6.7.17. При наличии жалобы со стороны Клиента о неполучении Перевода, если Переводу в Системе присвоен статус выплаченного Перевода и на основании запроса Оператора Системы, отправленного любым доступным способом, Участник-получатель не предоставляет Оператору Системы документ, подтверждающий факт выплаты и содержащий собственноручную или электронную подпись Получателя в течение 3-х рабочих дней с момента отправки запроса, то Оператор Системы имеет право изменить статус Перевода в Системе на успешный и направить Расчетному центру в составе Реестра распоряжение на списание в порядке, не требующем дополнительного распоряжения Участника, сумму Перевода и сумму комиссии за него, уплаченную Участнику-получателю Оператором Системы, со Счета Участника-получателя.

6.7.18. Если Участник-получатель не завершил процедуру оформления выплаты Перевода, направленного для выплаты наличными денежными средствами в страну, Участники которой осуществляют выплаты таких Переводов по безадресной технологии, в течение времени, определенного Оператором Системы, Оператор считает такой Перевод невыплаченным и имеет право программным способом изменить статус такого Перевода на успешный для предоставления возможности выплаты данного Перевода стандартным способом любым вышеупомянутым Участником Системы. Период, по истечении которого изменяется статус, определяется и изменяется Оператором Системы в одностороннем порядке. Оператор Системы вправе, но не обязан информировать Участников Системы о временных характеристиках данного периода.

7. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖНОГО КЛИРИНГА И РАСЧЕТОВ

7.1. Порядок осуществления платежного клиринга

7.1.1. Расчеты по операциям, совершенным Отправителем Участника в целях перевода денежных средств осуществляется со Счета этого Участника.

7.1.2. Платежный клиринг в Платежной системе осуществляется Платежным клиринговым центром посредством:

- выполнения процедур приема к исполнению Распоряжений Участников, включая проверку соответствия Распоряжений установленным требованиям, определение достаточности денежных средств для исполнения Распоряжений Участников и определение платежных клиринговых позиций;
- передачи Расчетному центру Реестра для исполнения принятых Распоряжений Участников, в том числе для списания и(или) зачисления по Счету ЦПКК (по необходимости);
- направления Участникам извещений (подтверждений), касающихся приема к исполнению Распоряжений Участников, а также передачи извещений (подтверждений), касающихся исполнения Распоряжений Участников.

7.1.3. Процедуры приема к исполнению Распоряжений Участников, осуществляемые Платежным клиринговым центром, включают в себя:

- удостоверение права распоряжения денежными средствами, которое осуществляется посредством проверки электронной подписи, и (или) кодов, паролей, иных средств, позволяющих подтвердить, что Распоряжение в электронном виде подписано Участником;
- контроль целостности Распоряжений в электронном виде, который осуществляется Платежным клиринговым центром посредством проверки неизменности реквизитов Распоряжения;
- структурный контроль Распоряжений в электронном виде, который осуществляется Платежным клиринговым центром посредством проверки установленных реквизитов и максимального количества символов в реквизитах Распоряжения;
- контроль значений реквизитов Распоряжений, который осуществляется путем значений реквизитов Распоряжений, их допустимости и соответствия;
- контроль достаточности денежных средств при совершении каждой операции.

7.1.4. Передача представленных к оплате операций осуществляется Платежным клиринговым центром до 14:00 часов по московскому времени рабочего дня, следующего за операционным/-и днем/днями.

7.1.5. Определение платежной клиринговой позиции Прямого участника по общему правилу осуществляется на валовой основе с учетом применения Тарифов и согласно Временному регламенту. По соглашению Оператора с Участником платежная клиринговая позиция по всем и(или) отдельным переводам денежных средств Участника может определяться на нетто-основе.

7.1.6. Платежная клиринговая позиция на валовой основе за операционный день определяется в разрезе валют в размере общей суммы подлежащих исполнению Распоряжений Участников, по которым Участник является плательщиком, и общей суммы Распоряжений Участников, по которым Участник Платежной системы является получателем средств, а также общей суммы комиссии, подлежащей списанию и(или) зачислению Участникам. Платежная клиринговая позиция на нетто-основе, в случае ее применения, определяется в размере разницы между общей суммой подлежащих исполнению Распоряжений Участников за операционный день, по которым Участник является плательщиком, и общей суммой Распоряжений Участников, по которым Участник является получателем средств.

7.1.7. При определении платежной клиринговой позиции Прямого участника учитываются платежные клиринговые позиции Косвенных участников, Партнеров, БПА/БПСА. Платежный клиринговый центр предоставляет информацию о текущей платежной клиринговой позиции Прямого

участника с учетом платежной клиринговой позиции Косвенного участника, Партнера, БПА/БПСА, для осуществления расчетов с Расчетным центром.

7.1.8. Платежные клиринговые позиции Участников формируются в валюте совершения операции:

- в рублях РФ – по операциям в рублях РФ;
- в долларах США – по операциям в долларах США;
- в ЕВРО – по операциям в ЕВРО;
- в иной иностранной валюте – по операциям в соответствующей иной иностранной валюте.

7.1.9. Платежный клиринговый центр для осуществления расчетов в рамках Системы отправляет в Расчетный центр Распоряжения Участников с указанием их платежных клиринговых позиций (и при необходимости привлеченных ими для работы в Системе третьих лиц), в том числе для осуществления списания и(или) зачисления по Счету ЦПКК, а также распоряжение Платежного клирингового центра для осуществления расчетов с Операторами УПИ и Оператором в форме Реестра.

7.2. Порядок осуществления расчетов

7.2.1. Участник обеспечивает на своем Счете Участника денежные средства в размере, достаточном для проведения расчетов по операциям, инициированным Отправителями Участника, в том числе Отправителями Косвенного участника, Партнера, БПА/БПСА.

7.2.2. При определении достаточности денежных средств на Счете Участника для проведения Операций учитываются все суммы Распоряжений, отправленных Участником (в том числе Косвенными участниками, БПА/БПСА, Партнерами), и Распоряжений, направленных в адрес Участника (Косвенных участников, его БПА/БПСА, Партнеров) и/или все суммы выплаченных Участником (Косвенных участников, его БПА/БПСА, Партнеров) Переводов.

7.2.3. При отсутствии достаточных денежных средств на Счете Участника либо при отсутствии установленного Оператором Системы расходного Лимита, или при отрицательном результате иных процедур приема к исполнению Распоряжения Участника, Оператором Системы такое Распоряжение к исполнению не принимается.

7.2.4. Возможность, а также порядок осуществления расчетов с предоставлением недостающих средств Расчетным центром, в котором открыты Счета Участников, определяется Расчетным центром по согласованию с Оператором Системы. Размер расходного Лимита определяется Расчетным центром на основе анализа финансового состояния Участника и иных факторов и доводится до его сведения, в случае установления Лимита, по Согласованным каналам связи либо путем направления электронного документа в порядке, предусмотренном договором с Расчетным центром. Информация об установлении Участнику увеличенного доступного Лимита незамедлительно предоставляется Расчетным центром в Платежный клиринговый центр.

7.2.5. Порядок и условия открытия Счетов Прямых участников определяются Расчетным центром и не являются предметом регулирования настоящих Правил. Порядок и условия открытия Счетов Косвенных участников (в случае их открытия) или условия отдельного договора, регламентирующего порядок взаиморасчетов по операциям, совершенным Косвенным участником в Системе, определяются Прямыми участниками с учетом положений настоящих Правил. В случае любых несоответствий между настоящими Правилами и договором между Участником и Расчетным (Прямым участником) центром преимущественную силу имеют положения Правил.

7.2.6. Прямой участник и (или) ПКЦ, выполняющий функции ЦПКК, предоставляет Расчетному центру право на основании заранее данного акцепта списывать/зачислять со Счета Участника и(или) Счета ЦПКК денежные суммы для проведения расчетов в рамках Платежной системы. Косвенный участник в случае открытия банковского счета у Прямого участника предоставляет Прямому участнику право на основании заранее данного акцепта списывать со Счета Косвенного участника денежные суммы для проведения расчетов в рамках Системы.

7.2.7. Расчет в Платежной системе осуществляется Расчетным центром посредством списания и зачисления денежных средств по Счетам Прямых участников и (или) по Счетам ЦПКК на основании поступившего от Платежного клирингового центра Реестра.

7.2.8. В случае недостаточности денежных средств на Счете Прямого участника, открытом в Расчетном центре в валюте операции, сумма, эквивалентная возникшей задолженности, списывается со Счета Прямого участника, открытого в Расчетном центре в иной валюте.

7.2.9. Порядок использования денежных средств в иных валютах для осуществления расчетов Косвенных участников по счетам, открытым у Прямого участника, в случае недостаточности денежных средств на Счетах Косвенного участника определяется Прямым участником.

7.2.10. Участник на основании полученного Отчета и (или) Партнеры, БПА, БПСА (в случае получения ими Отчетов) осуществляют сверку расчетов по операциям с Клиентами, проведенным в Системе. В случае обнаружения расхождений в данных, содержащихся в Отчете, с данными Участника (в том числе по операциям привлеченных им Косвенных участников, Партнеров, БПА, БПСА) и (или) с данными самих Косвенных участников, Партнеров, БПА, БПСА, последние обязаны незамедлительно, но не позднее 14:00 дня поступления Отчета урегулировать спорные вопросы с Платежным клиринговым центром и(или) Прямым участником и Платежным клиринговым центром. В случае если мероприятия, проводимые для урегулирования спорных вопросов, не могут быть завершены до 14:00 дня поступления Отчетов, расчеты за операционный день проводятся по данным, содержащимся в Отчетах, первоначально поступивших от Платежного клирингового центра, при этом расчеты по выявленным расхождениям осуществляются не позднее рабочего дня, следующего за днем завершения мероприятий по урегулированию расхождений. До урегулирования расхождений, выявленных при осуществлении сверки расчетов по осуществленным операциям, риск возврата денежных средств Отправителям по операциям, в отношении которых Участник не получил подтверждение Операционного центра о возможности его возврата, несет Участник. В этом случае Участник безусловно обязан возместить денежные средства по такой операции, включая вознаграждения иных Субъектов Системы.

7.2.11. Денежные средства, находящиеся на Счете Участника, открытом для участия в Системе, и (или) Счете ЦПКК могут быть использованы для целей:

- осуществления расчетов по операциям, разрешенным в Системе;
- оплаты вознаграждения Оператора, Операционного центра, Платежного клирингового центра, Расчетного центра, комиссий Участников в соответствии с действующими в Системе Тарифами;
- возмещения сумм задолженности, причитающихся Оператору Системы и (или) Расчетному центру, за исключением вознаграждения, и (или) ЦПКК;
- осуществления перевода остатка денежных средств, находящихся на Счетах, в связи с закрытием Счетов, на иной счет Участника, при условии урегулирования расчетов в рамках Системы.

7.2.12. Денежные средства, находящиеся на Счетах Участника, не могут быть использованы Участником для осуществления иных целей, кроме указанных в пункте 7.2.11 Правил, если иное не будет предусмотрено договором об открытии банковского счета между Прямым/Косвенным участником и Расчетным центром/Прямым участником.

7.2.13. Расчетный центр исполняет Распоряжения Прямого участника (не противоречащие действующему законодательству Российской Федерации) по перечислению денежных средств путем списания и зачисления по Счетам Участников и(или) Счетам ЦПКК, открытых в Расчетном центре, в пределах остатков денежных средств на Счете/Счетах и установленных Лимитов.

7.2.14. Расчетный центр осуществляет урегулирование позиций Участников и списание и(или) зачисление по Счету ЦПКК после получения Реестра от Платежного клирингового центра в сроки, определенные Временны́м регламентом Платежной системы.

7.2.15. Платежный клиринговый центр осуществляет установку и контроль Лимита Участника. Установка Лимита Участника осуществляется с учетом расходного лимита. Прямой Участник и(или) ЦПКК[1] поручает Расчетному центру предоставлять Платежному клиринговому центру данные об остатках на Счете. Данные предоставляются в соответствии с договором Оператора с Расчетным центром.

7.2.16. Лимит Участника устанавливается в валюте Счета ежедневно по рабочим дням.

7.2.17. Контроль Лимита Участника осуществляется Платежным клиринговым центром путем отслеживания в режиме реального времени суммы авторизационных запросов. Лимит Участника уменьшается по дебетовым операциям и увеличивается по кредитовым операциям на сумму Перевода и вознаграждения Субъектов по каждой успешно проведенной авторизации в соответствии с технологией Системы.

7.2.18. Расчеты и платежный клиринг производятся согласно Временно́му регламенту за закрытый отчетный период.

7.2.19. Для подтверждения правильности расчетов с Прямыми участниками, открывшими Счета в Расчетном центре, и находящимися у них на обслуживании, Оператор Системы высылает им Отчет, содержащий платежно-клиринговую позицию Участника об исполненных операциях (Распоряжениях), включая операции Косвенных участников, Партнеров, а также БПА (БПСА) в рамках Платежной системы не позднее следующего рабочего дня после проведения Расчетным центром взаиморасчетов по Распоряжениям за операционный(-ые) день (дни), предшествующий(-ие) дню расчетов. В целях подтверждения правильности расчетов по Счетам ЦПКК Оператор формирует и направляет ЦПКК документы, предусмотренные договором Оператора с ЦПКК.

7.2.20. Расчеты с Косвенными участниками Прямые участники, у которых на обслуживании находятся соответствующие Косвенные участники (включая Иных Косвенных участников, которые работают без открытия банковских счетов у Прямых участников) осуществляют самостоятельно.

7.3. Временно́й регламент осуществления платежного клиринга и расчетов

7.3.1. Операционный центр осуществляет прием и обработку Распоряжений Клиентов ежедневно с 00:00:00 до 23:59:59 часов по московскому времени.

7.3.2. В качестве единой шкалы времени при осуществлении платежного клиринга и расчетов в Платежной системе признается московское время.

7.3.3. Рабочими днями Расчетного центра являются рабочие дни, установленные законодательством Российской Федерации.

7.3.4. Функции Операционного центра по приему и обработке Распоряжений Клиентов и Участников, а также функции Платежного клирингового центра по проверке возможности осуществления операций Участниками осуществляются ежедневно с 00:00:00 до 23:59:59 часов (за исключением вынужденных технологических перерывов).

7.3.5. Оператор контролирует соблюдение следующих временны́х интервалов при формировании платежно-клиринговых позиций и проведении расчетов:

Регламентные работы	Временной интервал	Исполнитель
День 1		
Прием и обработка Распоряжений Клиентов/Участников	с 00:00:00 до 23:59:59	Операционный центр

[1] В случае открытия Счета в Расчетном центре.

Передача обработанных Распоряжений Участников в Платежный клиринговый центр		
Проверка возможности осуществления операций	с 00:00:00 до 23:59:59	Платежный клиринговый центр
День 2[1]		
Формирование платежно-клиринговой позиции Участников и Отчета по операциям ЦПКК за закрытый отчетный период	с 00:00:00 до 11:00:00	Платежный клиринговый центр
Предоставление Отчетов Участников, Отчета по операциям ЦПКК и Реестра за закрытый отчетный период	до 14:00:00	Платежный клиринговый центр
Проведение расчетов за закрытый отчетный период и информирование Платежного клирингового центра о проведении расчетов между Участниками и(или) по Счетам ЦПКК	до 17:00:00 *	Расчетный центр

* *Допускается отклонение от установленного регламентного времени не более чем на 30 (тридцать) минут для завершения обмена информацией между Расчетным центром и Платежным клиринговым центром*.

7.3.6. Формирование платежно-клиринговой позиции Участников, Отчета по операциям ЦПКК (по необходимости), передача Отчетов Участникам и(или) ЦПКК (по необходимости) и Реестра в Расчетный центр, расчёты – проводятся ежедневно в соответствии с Таблицей:

День приёма Распоряжения от Клиента/Участника	**День передачи, обработки Распоряжения Участника**	**День исполнения Распоряжения Участника**	**День направления Отчетов Участников, Отчета по операциям ЦПКК и Реестра[2]**	**День информирования Участника о произведенных расчетах путем направления Отчета об исполнении распоряжений[3]**
Понедельник	Понедельник	Вторник	Вторник	Не позднее среды
Вторник	Вторник	Среда	Среда	Не позднее четверга
Среда	Среда	Четверг	Четверг	Не позднее пятницы
Четверг	Четверг	Пятница	Пятница	Не позднее понедельника
Пятница	Пятница	Понедельник	Понедельник	Не позднее вторника
Суббота	Суббота	Понедельник	Понедельник	Не позднее вторника
Воскресенье	Воскресенье	Понедельник	Понедельник	Не позднее вторника

7.4. Порядок обеспечения исполнения обязательств Участников по переводу денежных средств

7.4.1. В целях обеспечения исполнения Участником своих финансовых обязательств по операциям перед Оператором, Операторами УПИ и другими Участниками, Участник обеспечивает размещение

[1] В случае, если День 2 выпадает на выходной (нерабочий) день в соответствии с действующим законодательством, регламентные работы проводятся в первый рабочий день, следующий за выходным (нерабочим) днем.

[2] Если день исполнения Реестра выпадает на выходной (нерабочий) день в соответствии с действующим законодательством, расчеты переносятся на ближайший рабочий день.

[3] Если день информирования Участников о произведенных расчетах выпадает на выходной (нерабочий) день в соответствии с действующим законодательством, информирование осуществляется в ближайший рабочий день.

на своем Счете в Расчетном центре сумму денежных средств, достаточную для проведения расчетов. Денежные средства, перечисленные на Счет Участника, могут быть по распоряжению Участника или на основании заранее данного акцепта переведены Расчетному центру в целях формирования Лимита Участника.

7.4.2. Платежный клиринговый центр реализует механизм обеспечения исполнения обязательств Участников путем авторизации операций только в пределах Лимита Прямого участника, информацию для формирования которого Платежный клиринговый центр получает от Расчетного центра.

7.4.3. Лимит Прямого участника формируется за счет денежных средств, перечисленных на Счета Участника, открытых в Расчетном центре, и постоянно меняется в зависимости от авторизуемых операций.

7.4.4. В случае осуществления расчетов в Системе на нетто-основе обеспечивается исполнение наибольшего по размеру обязательства Участника, что совместно с установкой и контролем Лимитов Участников обеспечивает гарантированное завершение расчетов.

7.4.5. Исполнение обязательств Участников Платежной системы по переводу денежных средств осуществляется Расчетным центром в пределах остатка денежных средств на Счетах Прямого участника на момент проведения расчетов, если иное не будет оговорено между Расчетным центром и Участником и доведено до сведения Оператора Системы дополнительно.

7.4.6. Расчетный центр передает в Платежный клиринговый центр информацию об остатках денежных средств на Счетах Прямых участников для формирования Лимитов Прямых участников и(или) информацию об остатках на Счетах ЦПКК (по необходимости), несет ответственность за своевременное оказание расчетных услуг в рамках Платежной системы в рамках установленных Лимитов.

7.4.7. Оператор системы вправе потребовать от Участника предоставления иного обеспечения исполнения обязательств способами, предусмотренными главой 23 ГК РФ.

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

7.5.1. Порядок оплаты услуг по переводу денежных средств и услуг платежной инфраструктуры и Оператора Платежной системы в рамках Платежной системы является единообразным для всех Участников Платежной системы.

7.5.2. Участники Платежной системы оплачивают услуги платежной инфраструктуры в соответствии с Тарифами Платежной системы (Приложение №3 к Правилам). Тарифы действуют с учетом требований законодательства стран местонахождения Участников, в т.ч. в отношении возможности использования определенных типов операций, валют, суммовых ограничений (возможны ограничения максимальной суммы единичного Перевода, максимальной суммы Переводов за определенный период и т.п.), применяемых форм расчетов.

7.5.3. Общие принципы оплаты Услуг:

7.5.3.1. Если иное не указано дополнительно, вознаграждение уплачивает Клиент, получающий Услуги Системы: физическое лицо или юридическое лицо/индивидуальный предприниматель;

7.5.3.2. Размер вознаграждения, уплачиваемого Клиентом, включает в себя вознаграждение всех субъектов, участвующих в осуществлении перевода денежных средств: Участника-отправителя, Оператора Системы, Операторов УПИ, Участника-получателя, а также посредников в переводе (при их наличии);

7.5.3.3. При обслуживании Клиента:

- вознаграждение взимается в полном объеме Участником, обслуживающим Клиента, и одновременно:

- Участник уплачивает вознаграждение Оператору Системы за оказание услуг Оператора Системы и услуг платежной инфраструктуры в размере, определяемом Оператором Системы, а также вознаграждение, причитающееся иным Участникам. В результате в распоряжении Участника остается вознаграждение, являющееся доходом Участника, в размере, указанном в Приложении №3 к Правилам (Комиссия Участника-отправителя);
- Участник, выступающий в качестве Участника-получателя, по каждому совершенному переводу денежных средств сверх его суммы получает вознаграждение за услуги по переводу денежных средств в размере, установленном Оператором Системы в качестве Тарифов Системы (Приложение №3 к Правилам - Комиссия Участника-получателя);

7.5.3.4. Процедуры расчета и уплаты комиссии Оператору/Оператором Системы осуществляются Операторами УПИ в рамках общих процедур клиринга и расчетов, в частности, суммы вознаграждения включаются в платежную клиринговую позицию по каждому Участнику;

7.5.3.5. По общему правилу по Бивалютным переводам вознаграждение Участникам выплачивает Оператор Системы или Участник-получатель, включая оператора платежной системы, с которой Оператор осуществляет межсистемное взаимодействие.

7.5.4. Общие принципы установления тарифов для физических лиц:

7.5.4.1. Тарифы для физических лиц признаются тарифами для обслуживания физических лиц каждого Участника, оказывающего Услуги Системы;

7.5.4.2. Порядок оплаты услуг, размер вознаграждения определяется Оператором Системы;

7.5.4.3. Допускается самостоятельное установление индивидуальных тарифов для Отправителей – физических лиц Участником-отправителем в случаях использования при обслуживании Отправителей различных средств ДБО, банковских счетов, при привлечении Партнеров, БПА (БПСА);

7.5.4.4. Тарифы для физических лиц указаны в Приложении №3 к настоящим Правилам. Дополнительно тарифы для физических лиц, а также информация об особенностях и существующих ограничениях при отправке/выдаче Перевода размещается на официальном сайте Оператора в сети Интернет;

7.5.4.5. Тарифы для физических лиц, а также самостоятельно установленные в соответствии с подпунктом 7.5.4.3 настоящего пункта тарифы Участника доводятся до Клиентов, обслуживаемых Участником (в том числе привлеченными им Партнерами, БПА/БПСА), в порядке, устанавливаемом Участником;

7.5.4.6. В связи с наличием возможности варьирования комиссионного вознаграждения в соответствии с подпунктом 7.5.4.5 настоящего пункта точный размер комиссионного вознаграждения доводится до сведения Отправителя в местах обслуживания Клиентов Участников, их Партнеров, БПА, БПСА, на дисплеях терминалов самообслуживания, с помощью систем ДБО.

7.5.5. Общие принципы определения комиссионного вознаграждения (далее – «комиссия»):

- комиссия взимается сверх суммы перевода денежных средств. По трансграничным переводам комиссия может быть удержана из суммы перевода денежных средств;
- комиссия может быть выражена:
  - в процентном отношении к сумме Перевода или к сумме комиссии, взимаемой с Клиента, получающего Услуги Системы;
  - в процентном отношении к сумме Перевода или к сумме комиссии, взимаемой с Клиента, получающего Услуги Системы, плюс фиксированная сумма;

- в фиксированной сумме;

- размер комиссии может варьироваться, в том числе в зависимости:
  - от суммы Перевода;
  - от направления Перевода;
  - от используемых Отправителем средств осуществления Перевода, в том числе валюты, Электронных средств платежа и форм безналичных расчетов;
  - от выбранного Отправителем места осуществления Перевода: в офисах Участника, Партнера, БПА, БПСА, с использованием средств ДБО и т.п.;
  - от способа доставки Перевода Получателю;
  - от различий валюты отправки Перевода и валюты выдачи Перевода Получателю;
  - от наличия/отсутствия дополнительных, сопутствующих Переводу, услуг;
  - от наличия/отсутствия посредников в Переводе;
  - от категории Получателя – поставщика услуги;
- максимальный размер комиссии может быть ограничен фиксированной суммой;
- сумма комиссии округляется по правилам, установленным Оператором Системы.

Валюта взимания комиссии определяется Участником самостоятельно.

7.5.6. Оператор Системы имеет право устанавливать обменный курс, применяемый в Системе при осуществлении расчетов, как с Участниками Системы, так и с Клиентами. Обменный курс устанавливается, в том числе по переводам денежных средств при различии валюты, предоставленной Отправителем – физическим лицом, и валюты переводимых и/или выплачиваемых денежных средств Получателю, а также при осуществлении иных операций, устанавливаемых Оператором Системы, порядок и условия совершения которых предполагают осуществление расчетов с использованием различных валют. При этом:

7.5.6.1. Обменный курс фиксируется в ПО Системы для каждой транзакции в момент совершения[1] Бивалютного перевода, таким образом, при выдаче и в рамках расчетов с Участником Получателя обменные курсы по транзакции не изменяются и сохраняются равными курсам, установленным при отправке.

7.5.6.2. Округление обменных курсов, устанавливаемых Оператором, осуществляется по математическому методу.

7.5.6.3. Обменный курс или информация о сумме выплаты перевода в валюте, отличной от валюты Перевода, доводится до сведения Отправителя в местах обслуживания клиентов Участников, их Партнеров, БПА, БПСА, на дисплеях банкоматов, терминалов самообслуживания, с помощью систем ДБО.

7.5.6.4. Обменный курс доводится до сведения Участников (включая привлеченных им Партнеров, БПА, БПСА) в ПО Системы.

7.5.7. Порядок оплаты услуг платежной инфраструктуры для всех категорий Субъектов Платежной системы отражаются в договорах с Оператором.

7.5.8. Сумма комиссионного вознаграждения, взимаемая с Отправителя по конкретной операции при оказании услуг по переводу денежных средств, доводится до сведения Отправителя в местах обслуживания Клиентов Участников, их Партнеров, БПА, БПСА, на дисплеях банкоматов, терминалов самообслуживания, с помощью систем ДБО до момента осуществления операции.

[1] Подтверждением наличия перевода в ПО Системы является успешный статус Перевода.

7.5.9. Запрещено устанавливать минимальный размер оплаты услуг по переводу денежных средств Участниками и их Клиентами.

7.5.10. Общий порядок расчета вознаграждения Участника-отправителя в случае взимания комиссии с Отправителя:

- вознаграждение Участника-отправителя рассчитывается, как разница между комиссией, полученной с Отправителя, и комиссией, подлежащей списанию со Счета Участника-отправителя для оплаты вознаграждения Участнику-получателю (в том числе являющемуся участником или расчетным центром платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие) и Оператору Системы, и остается в его распоряжении, если иное не предусмотрено соответствующим договором с Оператором Системы;
- вознаграждение вычисляется в валюте операции в процентном выражении от суммы операции или суммы комиссии, взимаемой с Отправителя;
- полученное вознаграждение округляется[1] до 2-х знаков после запятой;
- вознаграждение, подлежащее списанию со счета Участника-отправителя, вычисляется в валюте операции;
- в случае если вознаграждение помимо процентного выражения содержит и фиксированную сумму, фиксированная часть вознаграждения прибавляется к процентной части, вычисленной вышеуказанным способом;
- в случае уплаты вознаграждения только в виде фиксированной суммы, вознаграждение Участника-отправителя фиксируется в Тарифах Системы;
- в случае отличия валюты расчетов по вознаграждению от валюты операции рассчитанные суммы соответствующего вознаграждения умножаются на обменный курс и результат умножения округляется до 2-х знаков после запятой.

7.5.11. В случае если при расчете вознаграждения в процентном выражении от суммы операции или суммы комиссии, взимаемой с Отправителя (или процентном выражении плюс фиксированная часть), в Тарифах устанавливается максимальное ограничение вознаграждения Участника-отправителя в виде доли от комиссии, уплачиваемой Отправителем, то порядок расчета его вознаграждения следующий:

- вознаграждение Участника-отправителя вычисляется в валюте операции в процентном выражении от суммы операции или суммы комиссии, взимаемой с Отправителя, но не более чем сумма, вычисленная исходя из максимального ограничения в виде доли от комиссии, уплачиваемой Отправителем, и также при необходимости округляется до 2-х знаков после запятой;
- в случае если вознаграждение помимо процентного выражения содержит и фиксированную сумму, фиксированная часть вознаграждения прибавляется к сумме, вычисленной в процентном выражении от суммы Перевода или суммы комиссии, взимаемой с Отправителя, при этом итоговая сумма вознаграждения Участника-отправителя не должна превышать сумму, вычисленную исходя из максимального ограничения в виде доли от комиссии, уплачиваемой Отправителем;
- в случае отличия валюты расчетов по вознаграждению от валюты операции рассчитанная сумма комиссии Участника-отправителя умножается на обменный курс и результат умножения округляется до 2-х знаков после запятой;
- вознаграждение в валюте операции, подлежащее списанию со счета Участника-отправителя, вычисляется как разница между комиссией, уплачиваемой Отправителем, и рассчитанной вышеуказанным способом вознаграждением Участника-отправителя.

[1] Здесь и далее: округление в Системе осуществляется по математическому методу.

7.5.12. Общий порядок расчета комиссионного вознаграждения Участников в случае, когда комиссия с Отправителя - физического лица не взимается в соответствии с Тарифами Оператора:

- Участник-получатель (в том числе являющийся участником или расчетным центром платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие) или Участник-отправитель уплачивает комиссионное вознаграждение Оператору Системы и Участнику-отправителю или Участнику-получателю соответственно за прием Распоряжения Клиента об осуществлении перевода денежных средств, выдачу (зачисление) Перевода Получателю через Систему;
- вознаграждение Участникам, в том числе за осуществление Бивалютных переводов, обменные курсы для которых устанавливаются Оператором Системы, может также выплачивать Оператор Системы. В случае если плательщиком вознаграждения за осуществление Участниками Бивалютных переводов выступает Оператор Системы, оплата указанного вознаграждения Субъектам Платежной системы осуществляется Расчетным центром на основании распоряжения Платежного клирингового центра, содержащего платежную клиринговую позицию соответствующего Участника в соответствующей валюте и вознаграждение Оператора и Расчетного центра (при наличии), путем зачисления денежных средств на Счет Участника и(или) на Счет ЦПКК. Бухгалтерское отражение вознаграждения Субъектов Платежной системы по Бивалютным переводам, обменные курсы для которых устанавливаются Оператором Системы, осуществляется Оператором Системы в рублях РФ по обменному курсу, действующему на момент отправки Бивалютного перевода;
- вознаграждение в валюте операции вычисляется в процентном выражении;
- полученное вознаграждение округляется до 2-х знаков после запятой;
- в случае если вознаграждение помимо процентного выражения содержит и фиксированную сумму, фиксированная часть вознаграждения прибавляется к процентной части, вычисленной вышеуказанным способом;
- в случае уплаты вознаграждения только в виде фиксированной суммы, вознаграждение, подлежащее уплате Участнику, фиксируется в Тарифах Системы;
- в случае отличия валюты расчетов по вознаграждению от валюты операции рассчитанная сумма вознаграждения умножаются на обменный курс и результат умножения округляется до 2-х знаков после запятой.

7.5.13. Общий порядок расчета вознаграждения Участника-получателя в случае взимания комиссии с Отправителя:

- Участник-отправитель (в том числе являющийся участником или расчетным центром платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие) выплачивает вознаграждение Оператору Системы и Участнику-получателю за участие в Переводе (окончательную доставку денежных средств Получателю). Вознаграждение Участнику-получателю может выплачиваться Оператором Системы;
- вознаграждение в валюте операции вычисляется в процентном выражении от суммы операции или суммы комиссии, взимаемой с Отправителя, но не более чем сумма, вычисленная исходя из максимального ограничения в виде доли от комиссии, уплачиваемой Отправителем, при наличии такого ограничения;
- полученное вознаграждение округляется до 2-х знаков после запятой;
- в случае если вознаграждение помимо процентного выражения содержит и фиксированную сумму, фиксированная часть вознаграждения прибавляется к сумме, вычисленной в процентном выражении от суммы операции или суммы комиссии, взимаемой с Отправителя, при этом итоговая сумма вознаграждения Участника-получателя не должна превышать сумму, вычисленную исходя из максимального ограничения в виде доли от комиссии, уплачиваемой Отправителем, при наличии такого ограничения;

– в случае уплаты вознаграждения только в виде фиксированной суммы, вознаграждение, подлежащее уплате Участнику, фиксируется в Тарифах Системы;

– в случае отличия валюты расчетов по вознаграждению от валюты операции рассчитанная сумма вознаграждения умножается на обменный курс и результат умножения округляется до 2-х знаков после запятой.

7.5.14. Если вознаграждение Участника-отправителя, Участника-получателя рассчитывается в процентном или смешанном выражении и при этом Оператором Системы установлен максимально допустимый размер комиссии, взимаемой с Отправителя – физического лица или уплачиваемой Участником, то по достижении данного максимально допустимого размера оно рассчитывается как вознаграждение, подлежащее уплате только в фиксированной сумме.

7.5.15. Расчеты по операциям, осуществленным Участниками (межбанковские платежи и межбанковские комиссии) и(или) списание (зачисление) по Счету ЦПКК осуществляются Расчетным центром ежедневно по рабочим дням на основании заранее данного акцепта и в соответствии с Реестром, предоставленным Платежным клиринговым центром, путем списания (зачисления) денежных средств с (на) Счета (Счет) Участника и(или) Счет ЦПКК, если иное не согласовано между Оператором Системы и Оператором УПИ и (или) Участником.

7.5.16. Оператор Системы получает вознаграждение от Участников Системы (в том числе являющихся участником или расчетным центром платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие) за исполнение функций Оператора, Операционного центра, Платежного клирингового центра, которая по общему правилу определяется, как разница между суммой комиссии, уплаченной Отправителем, и вознаграждением Участников.

7.5.17. Вознаграждение Оператора Системы за оказание операционных услуг и услуг платежного клиринга участникам расчетов по Бивалютным переводам в Платежной системе МАРЛИН, для осуществления которых обменные курсы устанавливаются Оператором Системы, определяется как разница между суммой Бивалютного перевода в валюте отправки и суммой Бивалютного перевода в валюте выдачи, пересчитанной в валюту отправки по обменному курсу, применяемому в Системе при проведении расчетов. Вознаграждение Оператора Системы выплачивается в порядке, предусмотренном абз. 3 п. 7.5.12 Правил, в рублях РФ.

7.5.18. Оплата Участниками услуг Оператора и услуг Операторов УПИ осуществляется по общему правилу ежедневно по рабочим дням на основании заранее данного акцепта и в соответствии с Реестром, предоставленным Платежным клиринговым центром, путем списания (зачисления) Расчетным центром денежных средств со (на) Счета (Счет) Участника, если иное не согласовано Оператором Системы и Оператором УПИ и (или) Участником. Вознаграждение за оказание услуг платежной инфраструктуры по операциям, совершенным Участниками в иностранной валюте (за исключением Бивалютных переводов, обменные курсы для которых устанавливаются Оператором Системы), выплачивается в рублях по курсу Банка России на дату осуществления операции.

7.5.19. В случае привлечения Оператором Расчетного центра размер и порядок уплаты комиссии (плата) за исполнение функций Расчетного центра определяется договором между Оператором и Расчетным центром.

7.5.20. Оператор Системы имеет право вносить изменения в Тарифы Системы, в т.ч. в одностороннем порядке менять размер комиссии, взимаемой с физического или юридического лица/индивидуального предпринимателя, размер платы за услуги платежной инфраструктуры и размер вознаграждения, уплачиваемого Оператором Системы Участникам за обслуживание Отправителей или Получателей. При этом Оператор Системы обязан заблаговременно направить Участнику информацию об изменениях.

7.5.21. Оператор Системы имеет право проводить различные акции лояльности и другие маркетинговые мероприятия, связанные с установлением соответствующего размера вознаграждения, направленные на продвижение Услуг Системы, стимулирование Участников и Клиентов Системы. Данные мероприятия могут иметь ограниченный срок действия, Оператор Системы имеет право в любой момент времени отменить, изменить условия проводимых акций, а также продлить срок

действия указанных мероприятий неограниченное количество раз. Информация о проводимых акциях доводится до Участников заблаговременно путем размещения ее в ЛК Участника в ПО Системы и (или) направления по Согласованным каналам связи.

7.6. Порядок оформления Актов оказанных услуг

7.6.1. Оператор Системы ежемесячно не позднее 15 (пятнадцатого) рабочего дня месяца, следующего за отчетным, формирует и направляет каждому Прямому Участнику Акт об оказании услуг к Договору участия (далее – «Акт участника») за отчетный месяц. Для Косвенного участника Оператор формирует Акт участника, содержащий сведения об операциях, совершенных Косвенным участником в Системе в течение отчетного месяца, и направляет его Прямому участнику и Косвенному участнику для осуществления расчетов между ними.

7.6.2. Прямой Участник не позднее 3 (трех) рабочих дней с даты получения Акта участника обязан направить Оператору Платежной системы подписанный Акт участника или мотивированный отказ от подписания Акта участника. Порядок и необходимость подписания Акта между Прямым и Косвенным участниками определяется ими самостоятельно. Акт участника подписывается Косвенным участником и Оператором в порядке, предусмотренном настоящим разделом в случае, если в течение отчетного месяца у Косвенного участника возникли денежные обязательства непосредственно перед Оператором, и наоборот. В иных случаях Акт участника между Косвенным участником и Оператором подписанию не подлежит.

7.6.3. В случае неполучения Оператором Системы подписанного Прямым участником Акта участника или оригинала мотивированного отказа от подписания Акта участника не позднее 20 (двадцатого) рабочего дня месяца, следующего за отчетным, услуги, полученные/оказанные Прямым участником (включая привлеченных им Косвенных участников, Партнеров, БПА (БПСА)) в рамках Системы, считаются оказанными/полученными надлежащим образом и полностью принятыми Прямым участником/Оператором Системы, а Акт участника считается подписанным Оператором Системы в одностороннем порядке.

7.6.4. Оформление ежемесячных Актов об оказании услуг к договорам с Операторами УПИ (далее – «Акт Оператора УПИ») осуществляется Оператором Системы в порядке, предусмотренном соответствующими договорами с Операторами УПИ.

7.6.5. Акты с Участниками и Операторами УПИ оформляются Оператором по состоянию на последнее число отчетного месяца. В случае если дата расторжения договора, заключенного с Участником или с Оператором УПИ, приходится на иной день, отличный от последнего числа отчетного месяца, Акт оформляется по состоянию на дату расторжения такого договора.

7.6.6. Вознаграждение Участника по Бивалютным переводам, обменные курсы для которых устанавливаются Оператором Системы, в Акте участника отражается в валюте отправки/выдачи Перевода и в рублях РФ по обменному курсу, действующему на момент отправки Бивалютного перевода. В случае необходимости составления акта сверки расчетов между Участником и Оператором его формирование осуществляется в валюте перевода (отправки/выдачи) и его эквивалента в рублях РФ по обменному курсу, применяемому в Системе для Участника.

7.6.7. Субъекты Системы вправе осуществлять обмен первичными бухгалтерскими документами путем их отправки почтой, нарочным, либо с использованием систем доверенных операторов электронного документооборота при условии использования Сторонами для подписания документов усиленных квалифицированных электронных подписей.

8. СОБЛЮДЕНИЕ ТРЕБОВАНИЙ ПО ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ, ПО ПРОТИВОДЕЙСТВИЮ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЕМ, И ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА (ПОД/ФТ), И СОПРОВОЖДЕНИЮ ПЕРЕВОДА СВЕДЕНИЯМИ ОБ ОТПРАВИТЕЛЕ

8.1. Принципы и условия обработки персональных данных Клиентов в Системе

8.1.1. Субъекты Системы являются самостоятельными операторами, организующими и осуществляющими обработку персональных данных, с учетом особенностей, предусмотренных настоящим разделом Правил. В соответствии с требованиями Федерального закона №152-ФЗ «О персональных данных» от 27.07.2006 г. (далее – «Закон №152-ФЗ») Субъекты Системы обязаны уведомить уполномоченный орган по защите прав субъектов персональных данных об осуществлении обработки персональных данных в случаях, предусмотренных законодательством РФ.

8.1.2. Принципы и условия обработки персональных данных Клиентов Субъектами Системы должны соответствовать требованиям законодательства РФ и Банка России. Участник самостоятельно, но с учетом положений Правил, определяет условия взаимодействия с привлеченными им лицами (Партнерами, БПА/БПСА) в части обработки персональных данных Клиентов – физических лиц.

8.1.3. Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (Субъекту ПДн).

8.1.4. В рамках Системы обработка персональных данных Клиентов – физических лиц осуществляется с учетом следующего:

8.1.4.1. Каждый Участник, обслуживающий Отправителя, выступает оператором персональных данных Отправителя. Каждый Участник, обслуживающий Получателя, является оператором персональных данных Получателя. Оператор и Операторы УПИ не являются операторами персональных данных Клиентов – физических лиц, за исключением случаев, предусмотренных Правилами, и осуществляют обработку персональных данных Клиента – физического лица по поручению соответствующего Участника. Участник, обслуживающий Отправителя, не является оператором персональных данных Получателя. Участник, обслуживающий Получателя, не является оператором персональных данных Отправителя.

8.1.4.2. Обработка персональных данных Клиента – физического лица, осуществляется в соответствии с принципами, установленными статьей 5 Закона №152-ФЗ, в целях и объемах, необходимых для:

- заключения и исполнения договора, в котором Клиент, как Субъект ПДн, является одной из сторон, в частности, для осуществления приема/выплаты переводов денежных средств, рассмотрения обращений Клиента – физического лица, иных технологических операций в рамках Системы;
- соблюдения требований законодательства РФ;
- информирования физического лица об Услугах Системы, об услугах Оператора Системы и Участников;
- участия физического лица в акциях лояльности и других мероприятиях по продвижению Услуг Системы, услуг Оператора Системы и Участников, в т. ч. с привлечением третьих лиц.

8.1.4.3. Обработка персональных данных осуществляется с согласия Клиентов – физических лиц: совместно с заявлением на Перевод и на выдачу Перевода Участником, обслуживающим Клиента, должно быть получено согласие Клиента – физического лица на обработку его персональных данных, на поручение обработки своих персональных данных Оператору, Операторам УПИ, способами, указанными в п. 8.1.5 Правил. При отсутствии согласия на обработку персональных данных Клиента (отказ Клиента предоставить такое согласие),

Перевод не принимается к исполнению и(или) не выдается. Участники Системы, использующие собственное программное обеспечение, в том числе средства интеграции с ПО Системы, обязаны самостоятельно реализовать получение согласия Субъектов ПДн – Клиентов Системы на обработку персональных данных, в т.ч. трансграничную передачу персональных данных).

8.1.4.4. К персональным данным Клиентов – физических лиц, обрабатываемым в целях осуществления переводов денежных средств, относится совокупность данных, позволяющая определить Субъекта ПДн, в т.ч.:

- фамилия, имя, отчество (при наличии);
- год, месяц, дата рождения;
- место рождения;
- адрес;
- реквизиты документа, удостоверяющего личность;
- реквизиты документа, подтверждающего право пребывания иностранного гражданина или лица без гражданства на территории РФ (при наличии);
- ИНН (при его наличии);
- СНИЛС (при его наличии);
- номер телефона и(или) электронный адрес;
- гражданство;
- резидентство.

8.1.5. Сторона, действующая в отношении обработки персональных данных Субъектов ПДн, указанных в п. 8.1.4 Правил, по поручению другой стороны, осуществляет обработку персональных данных как с использованием средств автоматизации, так и без их использования путем сбора, записи, систематизации, накопления, хранения, уточнения (обновления, изменения), извлечения использования, передачи, в том числе трансграничной, блокирования, удаления и уничтожения персональных данных с использованием баз данных, находящихся на территории Российской Федерации, за исключением случаев, предусмотренных действующим законодательством Российской Федерации. Сторона, действующая в отношении обработки персональных данных Субъектов ПДн, указанных в п. 8.1.4 Правил, по поручению другой стороны, не обязана получать согласие от Субъектов ПДн на обработку их персональных данных. Ответственность за получение согласия возлагается на сторону, предоставившую персональные данные Субъекту ПДн другой стороне.

8.1.6. Поручение на обработку персональных данных действует до даты расторжения договора Участника с Оператором или с Оператором УПИ.

8.1.7. Сторона, осуществляющая передачу персональных данных Субъекта ПДн другой стороне, гарантирует, что ею получено надлежащим образом оформленное согласие физических лиц на передачу и обработку персональных данных соответствующему Субъекту Системы, операторам иных платежных систем, с которыми Оператор установил межсистемное взаимодействие, в целях и в объеме, указанных в п. 8.1.4 Правил.

8.1.8. Обработка специальных категорий персональных данных (расовая, национальная принадлежность, состояние здоровья и т.п.), биометрических персональных данных в целях осуществления переводов денежных средств по Системе не осуществляется.

8.1.9. Стороны, задействованные в переводе денежных средств, обрабатывают персональные данные Клиентов – физических лиц в соответствии с требованиями национального законодательства, в том числе связанного с контролем в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, и настоящих Правил.

8.1.10. Применяемые для осуществления переводов денежных средств в Системе средства защиты информации должны обеспечивать конфиденциальность, целостность и подлинность электронных сообщений при осуществлении информационного обмена с Оператором Системы.

8.1.11. Стороны, в том числе действующие по поручению другой стороны, обязаны соблюдать меры по обеспечению безопасности и конфиденциальности персональных данных при их обработке, в т.ч. обеспечивать защиту персональных данных в соответствии с требованиями Закона №152-ФЗ.

8.1.12. Сторона, действующая при обработке персональных данных Субъекта ПДн по поручению другой стороны, обязуется по письменному запросу другой стороны в течение срока действия поручения на обработку персональных данных соблюдать требования, предусмотренные ст. 18.1, ст. 19 Закона №152-ФЗ, предоставлять документы и информацию, подтверждающие принятие мер и соблюдение требований, предусмотренных ст. 6 Закона №152-ФЗ; незамедлительно уведомлять другую сторону о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав Субъектов ПДн.

8.1.13. Сторона, действующая при обработке персональных данных Субъекта ПДн по поручению другой стороны, предупреждена о том, что эти данные могут быть использованы лишь в целях, для которых они сообщены. Сторона, передавшая персональные данные таких физических лиц, вправе требовать от получившей эти данные стороны подтверждения того, что это правило соблюдено.

8.1.14. Участники, созданные в соответствии с законодательством иностранного государства, обязаны также руководствоваться изложенными в настоящем разделе принципами и соблюдать требования законодательства своей инкорпорации в части сбора и обработки персональных данных.

8.1.15. Ответственность перед Субъектом ПДн несет сторона, являющаяся в отношении него оператором персональных данных. Лицо, осуществляющее обработку персональных данных по поручению оператора персональных данных Субъекта ПДн, несет ответственность перед оператором персональных данных этого Субъекта ПДн.

8.2. Принципы и условия осуществления деятельности в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Сопровождение перевода сведениями об Отправителе

8.2.1. Участники, а также привлеченные ими лица (далее в рамках данного раздела – «Участники и Партнеры») предпринимают все необходимые действия с целью противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма, экстремистской деятельности и финансированию распространения оружия массового уничтожения.

8.2.2. Участники и Партнеры, созданные в соответствии с законодательством Российской Федерации, при работе в Системе руководствуются Федеральным законом №115-ФЗ, а также международными актами о противодействии легализации (отмыванию) доходов, полученных преступным путем.

8.2.3. Участники и Партнеры, созданные в соответствии с законодательством иностранного государства, при работе в Системе руководствуются применимыми к ним нормативными актами страны регистрации, а также международными актами о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

8.2.4. Действия, направленные на противодействие легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма, экстремистской деятельности и финансированию распространения оружия массового уничтожения, в том числе включают в себя:

8.2.4.1. Разработку, утверждение правил внутреннего контроля в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма, экстремистской деятельности и финансированию распространения оружия массового уничтожения и программ осуществления контроля. Правила внутреннего контроля должны содержать порядок документального фиксирования необходимой информации, порядок

обеспечения конфиденциальности информации, квалификационные требования к подготовке и обучению кадров, а также критерии выявления и признаки необычных сделок.

8.2.4.2. Назначение специальных должностных лиц, ответственных за соблюдение и реализацию правил и программ, указанных в данном разделе.

8.2.4.3. Осуществление соответствующей уполномоченной службой в рамках системы внутреннего контроля проверки и оценки мероприятий в целях противодействия легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма, экстремистской деятельности и финансированию распространения оружия массового уничтожения.

8.2.4.4. Использование Участниками и Партнерами программного обеспечения для осуществления Переводов в Системе, содержащего следующий функционал:

- фиксирования сведений, полученных от Клиентов при совершении операций в Системе;
- передачи необходимых данных по всей цепочке платежа, содержащих в т.ч. уникальный номер операции;
- фиксирования дополнительных требований Участников-получателей в отношении идентификационных данных Клиентов Системы – физических лиц и/или ограничений по количеству и(или) сумме операций в отношении одного Отправителя или Получателя.

8.2.5. Одновременно с этим Участники и Партнеры Системы:

- не открывают счетов анонимным владельцам, не открывают счетов без личного присутствия лица, открывающего счет либо его представителя;
- не устанавливают и не поддерживают отношений с банками, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления;
- предпринимают меры, направленные на предотвращение установления отношений с банками, в отношении которых имеется информация, что их счета используются банками, не имеющими на территориях государств, в которых они зарегистрированы, постоянно действующих органов управления.

8.2.6. При осуществлении операций в Системе Участниками, созданными в соответствии с законодательством РФ, в случаях, предусмотренных Федеральным законом №115-ФЗ, проводится идентификация/упрощенная идентификация Клиента-физического лица.

8.2.7. Участники, созданные и осуществляющие деятельность в соответствии с законодательством, отличным от законодательства Российской Федерации, руководствуются применимым законодательством при определении случаев и способов идентификации, а также объема сведений, подлежащих установлению при ее проведении.

8.2.8. Сопровождение перевода денежных средств сведениями об Отправителе осуществляется Участником в случаях, предусмотренных Федеральным законом №115-ФЗ, если они не содержатся в Распоряжении Участника Платежной системы.

8.2.9. При отсутствии сведений об Отправителе, наличие которых требуется в соответствии с законодательством страны Участника-отправителя и/или Участника-получателя в сфере противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, Перевод считается не прошедшим проверку на соответствие установленным требованиям и в обработку Операционным центром не принимается. При приеме Перевода в обработку Оператор Системы обеспечивает техническую возможность сопровождения перевода денежных средств необходимыми сведениями и не несет ответственности за достоверность и полноту передаваемой информации.

9. СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ И ПОРЯДОК ОБЕСПЕЧЕНИЯ БЕСПЕРЕБОЙНОСТИ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ

9.1. Модель управления рисками

9.1.1. Система управления рисками в Платежной системе строится в соответствии с требованиями Федерального закона №161-ФЗ, Положения Банка России от 3 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») и Положения Банка России от 17 августа 2023 г. №821-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 № 821-П»).

9.1.2. Под системой управления рисками в Платежной системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для БФПС с учетом размера причиняемого ущерба.

9.1.3. В качестве организационной модели управления рисками в Системе принята модель распределения функций по оценке и управлению рисками между Оператором, Операторами УПИ и Участниками.

9.1.4. Оператор определяет требования к функционированию Участников и Операторов УПИ, выполнение которых обеспечивает бесперебойность функционирования Системы в целом.

9.1.5. Оператор непосредственно осуществляет координацию деятельности Субъектов Платежной системы, направленной на достижение, подтверждение и поддержание допустимого уровня рисков нарушения БФПС, под которыми понимается присущие функционированию Платежной системы типичные возможности неоказания, ненадлежащего оказания услуг Участникам вследствие наступления неблагоприятных событий, связанных с внутренними и внешними факторами функционирования Платежной системы.

9.1.6. Оператор осуществляет координацию деятельности Субъектов 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 исполнять и реализовать установленные мероприятия в рамках собственной системы управления рисками, руководствуясь требованиями настоящих Правил;
- Оператор контролирует исполнение настоящих Правил, в том числе:
  - устанавливает порядок информационного взаимодействия для управления рисками;
  - осуществляет постоянное взаимодействие с представителями Субъектов.

9.1.7. Рекомендации Оператора и (или) изменения в системе управления рисками размещаются Оператором по мере необходимости в ЛК или направляются по Согласованным каналам связи.

9.1.8. Оператор определяет формы осуществления контроля за соблюдением Субъектами порядка обеспечения БФПС.

9.1.9. Оператор осуществляет контроль за соблюдением Субъектами порядка обеспечения БФПС путем:

- анализа предоставляемой Субъектами информации в соответствии с порядком доведения до органов управления Оператора соответствующей информации о рисках, установленным настоящими Правилами;
- анализа полученных заявлений, обращений и жалоб Клиентов и/или Субъектов Системы.

9.1.10. Оператор определяет собственную структуру управления рисками и функциональные обязанности лиц и соответствующих структурных подразделений, ответственных за управление рисками.

9.1.11. Субъекты Системы самостоятельно организуют и осуществляют управление рисками, присущими их виду деятельности и участия в Системе. Система управления рисками каждого Субъекта Системы должна включать, но не ограничиваться, назначением ответственных сотрудников и (или) наделением соответствующими полномочиями подразделений, ответственных за управление рисками и разработкой внутренних правил по управлению рисками.

9.1.12. Субъекты Системы несут ответственность за реализацию системы управления рисками в их деятельности в соответствии с Правилами и требованиями законодательства Российской Федерации. Все Субъекты несут ответственность за управление рисками в пределах своих полномочий.

9.1.13. По осуществлению управления рисками устанавливается разграничение ответственности и полномочий между Субъектами.

9.1.13.1. Оператор:

- координирует деятельность Субъектов Системы по обеспечению БФПС;
- разрабатывает внутренние документы по управлению рисками в ПС и доводит их до сведения Субъектов;
- определяет мероприятия по управлению рисками;
- определяет и внедряет способы управления рисками, включая Риски ИБ;
- определяет показатели БФПС;
- осуществляет анализ рисков нарушения БФПС на основании первичной информации, предоставляемой Субъектами;
- устанавливает допустимый уровень рисков нарушения БФПС;
- контролирует соблюдение Субъектами Системы порядка обеспечения БФПС;
- выявляет текущие изменения присущего уровня риска нарушения БФПС;
- принимает меры, необходимые для достижения или поддержания допустимого уровня рисков нарушения БФПС;
- осуществляет информационное взаимодействие с Субъектами Системы в целях управления рисками нарушения БФПС.

9.1.13.2. Операционный центр:

- уполномочен и несет ответственность за управление операционным риском;
- обеспечивает уровень бесперебойности оказания операционных услуг в пределах стандартных значений, установленных Правилами;
- обеспечивает снижение риска нарушения бесперебойности оказания операционных услуг беспрерывной круглосуточной работой аппаратно-программных комплексов.

9.1.13.3. Платежный клиринговый центр:

- уполномочен и несет ответственность за управление кредитным риском и риском ликвидности;
- обеспечивает снижение риска нарушения БФПС путем исключения задержек времени окончания клирингового цикла, возникших по вине Платежного клирингового центра.

9.1.13.4. Расчетный центр:

- уполномочен и несет ответственность за управление расчетным риском (кредитным риском и риском ликвидности), в том числе создает организационную структуру управления кредитным

риском и риском ликвидности, а также разрабатывает внутренние нормативные документы, включая методики анализа кредитных рисков и рисков ликвидности в соответствии с условиями настоящих Правил;

- обеспечивает снижение риска нарушения БФПС исключением задержек времени проведения расчетов с Субъектами, возникших по вине Расчетного центра.

9.1.13.5. Участники:

- осуществляют соблюдение настоящих Правил, заключенных договоров, законодательства Российской Федерации;
- обеспечивают надлежащую защиту информации;
- обеспечивают поддержание необходимого остатка денежных средств на своих Счетах в Расчетном центре, а в случае формирования в отношении Участника расходного Лимита, обеспечивают своевременность исполнения денежных обязательств Участника перед иными Субъектами Системы.

9.1.14. Оценка эффективности системы управления рисками проводится Оператором на основании результатов мониторинга риска БФПС и построения профилей рисков с применением не менее чем одного метода из числа предусмотренных таблицей А.2 приложения А к национальному стандарту Российской Федерации ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска», утвержденному и введенному в действие приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2019 года №1405-ст «Об утверждении национального стандарта Российской Федерации» (М., ФГУП «Стандартинформ», 2020) (далее – «Стандарт»).

9.1.15. Оператор определяет профили рисков и меры, направленные на достижение и поддержание допустимого уровня риска нарушения БФПС. Меры управления рисками определяются на основании анализа событий риска за истекший период, потенциальных угроз внешней среды и прочих факторов.

9.1.16. В качестве экспертов выступают специалисты Оператора, привлеченные специалисты Субъектов, также могут привлекаться внешние эксперты.

9.1.17. В случае признания системы управления рисками эффективной, мероприятия по минимизации рисков следует также считать эффективными. В случае, если в течение анализируемого периода система управления рисками признана неэффективной, должны быть выработаны новые меры для достижения и поддержания допустимого уровня рисков БФПС.

9.1.18. Оператор обеспечивает проведение оценки системы управления рисками в Платежной системе, в том числе используемых методов оценки рисков в Платежной системе, результатов применения способов управления рисками в Платежной системе, не реже одного раза в 3 (три) года и документально оформляет результаты указанной оценки. При наличии коллегиального органа по управлению рисками в Платежной системе оценка системы управления рисками в Платежной системе должна проводиться данным органом.

9.1.19. Оператор вносит изменения в систему управления рисками в Платежной системе в случае, если действующая система управления рисками в Платежной системе не обеспечила 3 (три) и более раза в течение календарного года возможность восстановления оказания УПИ в течение периодов времени, установленных Оператором в Правилах Платежной системы, при их приостановлении.

9.1.20. Оператор при управлении рисками в Платежной системе оценивает риски, возникающие в связи с привлечением поставщиков (провайдеров), предоставляющих услуги в сфере информационных технологий в целях оказания Оператором УПИ услуг платежной инфраструктуры и (или) предоставляющих услуги обмена информацией при осуществлении операций с использованием Электронных средств платежа между операторами по переводу денежных средств и их клиентами и (или) между операторами по переводу денежных средств и иностранными поставщиками платежных услуг, предусмотренные п. 33 ст. 3 Федерального закона № 161-ФЗ (далее - поставщики услуг), в том числе обусловленные вероятностью невыполнения поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования

автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг.

9.2. Мероприятия системы управления рисками

9.2.1. Система управления рисками в Платежной системе предусматривает выполнение следующих мероприятий:

- определение организационной структуры управления рисками, обеспечивающей контроль за выполнением Субъектами требований к управлению рисками, установленных настоящими Правилами;
- определение мероприятий по управлению Риском ИБ в Платежной системе для операторов по переводу денежных средств, являющихся Участниками, и Операторов УПИ, а также определение для указанных Субъектов требований к обеспечению защиты информации для процессов, предусмотренных п. 10.1.5 Правил;
- определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;
- определение подразделения Оператора, осуществляющего управление Риском ИБ, в т.ч. обеспечивающее предъявление требований по управлению Риском ИБ к операторам по переводу денежных средств, являющихся Участниками, и к Операторам УПИ;
- доведение до органов управления Оператора Системы соответствующей информации о рисках;
- определение показателей БФПС в соответствии с требованиями нормативных актов Банка России;
- определение порядка обеспечения БФПС в соответствии с требованиями нормативных актов Банка России;
- определение методик анализа рисков в Системе, включая профили рисков, в соответствии с требованиями нормативных актов Банка России;
- 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.

9.2.2. Система управления Риском ИБ операторов по переводу денежных средств, являющихся Участниками Системы, и Операторов УПИ (далее – «СУР ИБ Участников и Операторов УПИ») должна отвечать следующим требованиям:

- СУР ИБ Участников и Операторов УПИ должна быть функционирующей;
- СУР ИБ Участников и Операторов УПИ должна соответствовать требованиям действующего законодательства Российской Федерации и нормативных актов Банка России;
- СУР ИБ Участников и Операторов УПИ должна предусматривать управление Риском ИБ при осуществлении ими операций в Платежной системе исходя из функций, выполняемых Участником и(или) Оператором УПИ в Платежной системе;
- Риск ИБ должен входить в состав операционного риска Участника и(или) Оператора УПИ;

- у Участника и(или) Оператора УПИ должна быть определена организационная структура по управлению Риском ИБ;
- Участником и(или) Оператором УПИ должны быть разработаны нормативные документы, описывающие порядок управления Риском ИБ с учетом требований настоящих Правил;
- Участником и(или) Оператором УПИ должно обеспечиваться формирование регулярной отчетности по инцидентам защиты информации и мерах реагирования и управления выявленными инцидентами защиты информации.

9.3. Организационная структура системы управления рисками Оператора

9.3.1. Управление рисками в Платежной системе осуществляется коллегиальным органом – Комитетом по управлению рисками. Председателем Комитета является единоличный исполнительный орган Оператора – Генеральный директор. В состав Комитета включаются ответственные за управление рисками представители Оператора Платежной системы, Операторов УПИ, Участников Платежной системы, а также, по согласованию с Банком России, могут быть включены представители Банка России с правом совещательного голоса.

9.3.2. Оператор Платежной системы и 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 Платежной системе.

9.3.3. В целях управления рисками в Платежной системе, в том числе обеспечения контроля за выполнением Субъектами требований к управлению рисками, установленных Правилами, задействована штатная организационная структура Оператора в соответствии с функциональными полномочиями органов и подразделений.

9.3.4. В организационную структуру управления рисками Оператора входит единоличный исполнительный орган и внутренние структурные подразделения Оператора. Должностные лица и органы управления Оператора имеют право затребовать от любого Оператора УПИ или Участника предоставления информации, предусмотренной Правилами.

9.3.5. Функциональные обязанности Комитета по управлению рисками:

- установление критериев оценки системы управления рисками в Платежной системе, включая системный риск;
- проведение оценки системы управления рисками в Платежной системе, в том числе используемых методов оценки рисков в Платежной системе;
- формирование предложений и рекомендаций по итогам проведения оценки системы управления рисками в Платежной системе.

9.3.6. Функциональные обязанности единоличного исполнительного органа Оператора по управлению рисками:

- утверждение основных принципов системы управления рисками;
- утверждение внутренних документов в области управления рисками;
- рассмотрение отчетов структурных подразделений о состоянии системы управления рисками и оценке принимаемых рисков;
- принятие необходимых управленческих решений по планированию мероприятий в случае признания уровня риска повышенным;
- разработка, применение и оценка эффективности методик анализа рисков в Системе, требования к оформлению и проверке результатов анализа.

9.3.7. Функциональные обязанности структурных подразделений Оператора по управлению рисками:

- разработка внутренних документов в области управления рисками;
- выбор и реализация мероприятий и способов достижения и поддержания допустимого уровня рисков в Системе, оценка их эффективности и совершенствования;
- установление предельных размеров (лимитов) обязательств Участников с учетом уровня рисков;
- мониторинг уровня рисков в Системе;
- анализ и регулярная оценка уровня риска по каждому из видов рисков;
- выявление, измерение и определение допустимого уровня риска по каждому из видов рисков;
- организация обмена информацией о рисках и мерах по управлению ими между структурными подразделениями Оператора;
- контроль за соблюдением всеми Участниками настоящих Правил;
- сбор, обработка и доведение до исполнительного органа по управлению рисками информации о рисках, в том числе информации, поступающей от Участников и Операторов УПИ.

9.4. Способы управления рисками

9.4.1. Оператор определяет способы управления рисками в Платежной системе, исходя из способов управления рисками, предусмотренных частью 5 статьи 28 Федерального закона №161-ФЗ (далее – «способы управления рисками в Платежной системе»).

9.4.2. Способы управления рисками в Платежной системе устанавливаются с учетом особенностей организации Платежной системы, модели управления рисками, процедур платежного клиринга и расчета, количества переводов денежных средств и их сумм, времени окончательного расчета.

9.4.3. В Системе применяются следующие способы управления рисками:

а) анализ Оператором документов Участников и Операторов УПИ, их деловой репутации;

б) получение сведений о привлекаемых Участниками Косвенных участниках, Партнерах, БПА и БПСА;

в) установление предельных размеров обязательств Участников (Лимитов Участников) в соответствии с учетом уровня риска;

г) управление очередностью исполнения Распоряжений Участников;

д) осуществление расчета в Системе до конца рабочего дня;

е) обеспечение возможности установления повышенного расходного Лимита или предоставления кредита финансово стабильным Участникам;

ж) проведение расчетов в Платежной системе в пределах предоставленных Участниками денежных средств;

з) моментальное изменение Лимитов Участников и доступных Лимитов при авторизации операции перевода денежных средств по распоряжениям Клиентов;

и) установление для Участников и Операторов УПИ ограничений по параметрам операций по осуществлению переводов денежных средств в случае выявления факта превышения пороговых значений показателей уровня Риска ИБ Участника Платежной системы, в том числе условия снятия таких ограничений.

9.5. Доведение до органов управления Оператора соответствующей информации о рисках

9.5.1. Информация о рисках в случае наступления чрезвычайных ситуаций или значительного нарушения допустимого уровня риска (включая случаи системных сбоев) незамедлительно доводится до сведения органов управления Оператора (Генерального директора).

9.5.2. Консолидированная информация обо всех произошедших рисках и об общем уровне рисков в Платежной системе доводится до сведения органов управления Оператора (Генерального директора) сотрудником, ответственным за управление рисками, по окончании плановой оценки всех рисков либо внеплановой оценки всех и(или) отдельных рисков в Платежной системе с использованием методик анализа рисков в Платежной системе, включая профили рисков. Информирование осуществляется в виде письменных отчетов сотрудника, ответственного за управление рисками Оператора.

9.6. Показатели бесперебойности функционирования Платежной системы

В соответствии с требованиями Положения Банка России №607-П определены следующие показатели БФПС.

9.6.1. Показатель продолжительности восстановления оказания услуг платежной инфраструктуры (далее – «показатель П1»), характеризующий период времени восстановления оказания услуг Операторами УПИ в случае приостановления оказания УПИ, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Банком России на основании ч. 3 ст. 27 Федерального закона №161-ФЗ.

Показатель П1 рассчитывается по каждому из Операторов УПИ и по каждому из инцидентов, повлекших приостановление оказания УПИ, как период времени с момента возникновения события, приведшего к приостановлению оказания УПИ в результате первого из возникших инцидентов, и до момента восстановления оказания УПИ.

При возникновении инцидентов, повлекших приостановление оказания УПИ одновременно двумя и более Операторами УПИ, показатель П1 рассчитывается как период времени с момента возникновения события, приведшего к приостановлению оказания УПИ в результате первого из возникших инцидентов, и до момента восстановления оказания УПИ всеми Операторами УПИ, у которых возникли инциденты.

Показатель П1 рассчитывается в часах/минутах/секундах.

9.6.2. Показатель непрерывности оказания УПИ (далее – «показатель П2») - период времени между двумя последовательно произошедшими в Платежной системе событиями, которые привели к нарушению оказания УПИ, соответствующего требованиям к оказанию услуг, в том числе вследствие нарушений требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее - инциденты), в результате которых приостанавливалось оказание УПИ. Приостановление (прекращение) участия в Платежной системе в случаях, предусмотренных Правилами Платежной системы в соответствии с пунктом 4 части 1 статьи 20 Федерального закона №161-ФЗ, не рассматривается в целях настоящего Положения в качестве инцидентов.

Показатель П2 рассчитывается по каждому из Операторов УПИ при возникновении каждого из инцидентов, повлекших приостановление оказания УПИ, как период времени между двумя последовательно произошедшими у Оператора УПИ инцидентами, в результате которых приостанавливалось оказание УПИ, с момента восстановления оказания УПИ, приостановленных в результате первого инцидента, и до момента возникновения события, приведшего к приостановлению оказания УПИ в результате следующего инцидента. Если Оператор УПИ оказывает в Платежной системе более одного вида УПИ одновременно, показатель П2 должен рассчитываться одновременно по всем видам УПИ, оказываемым данным Оператором УПИ.

Показатель П2 рассчитывается в часах/минутах/секундах.

9.6.3. Показатель соблюдения регламента (далее – «показатель П3») - соблюдение Операторами УПИ времени начала, времени окончания, продолжительности и последовательности процедур,

выполняемых Операторами УПИ 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 Федерального закона №161-ФЗ (далее – «регламент выполнения процедур»).

Показатель П3 рассчитывается по каждому Оператору УПИ. Для Операционного центра показатель П3 рассчитывается как отношение количества Распоряжений Участников Платежной системы (их Клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур, к общему количеству Распоряжений Участников Платежной системы (их клиентов), по которым были оказаны операционные услуги в течение календарного месяца, рассчитываемое по следующей формуле:

$$П3_{оц} = (N_{оц} / N_{оц}^{общ}) \times 100\ \%,$$

где:

$N_{оц}$ - количество Распоряжений Участников Платежной системы (их Клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур,

$N_{оц}^{общ}$ - общее количество Распоряжений Участников Платежной системы (их Клиентов), по которым были оказаны операционные услуги в течение календарного месяца.

Для Платежного клирингового центра показатель П3 рассчитывается как отношение количества Распоряжений Участников Платежной системы (их Клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур, к общему количеству Распоряжений Участников Платежной системы (их Клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца, рассчитываемое по следующей формуле:

$$П3_{пкц} = (N_{пкц} / N_{пкц}^{общ}) \times 100\ \%,$$

где:

$N_{пкц}$ - количество Распоряжений Участников Платежной системы (их Клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур,

$N_{пкц}^{общ}$ - общее количество Распоряжений Участников Платежной системы (их Клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца.

Для Расчетного центра показатель П3 рассчитывается как отношение количества Распоряжений Участников Платежной системы и (или) Платежного клирингового центра, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур, к общему количеству Распоряжений Участников Платежной системы и (или) Платежного клирингового центра, по которым были оказаны расчетные услуги в течение календарного месяца, рассчитываемое по следующей формуле:

$$П3_{рц} = (N_{рц} / N_{рц}^{общ}) \times 100\ \%,$$

где:

$N_{рц}$ - количество Распоряжений Участников Платежной системы и (или) Платежного клирингового центра, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур,

$N_{рц}^{общ}$ - общее количество Распоряжений Участников Платежной системы и (или) Платежного клирингового центра, по которым были оказаны расчетные услуги в течение календарного месяца.

Показатель П3 рассчитывается ежемесячно в процентах с точностью до двух знаков после запятой (с округлением по математическому методу).

Значение показателя П3 по Платежной системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем Операторам УПИ в отношении всех видов оказываемых ими услуг.

9.6.4. Показатель доступности Операционного центра Платежной системы (далее – «показатель П4») характеризует оказание операционных услуг Операционным центром Платежной системы.

Показатель П4 рассчитывается как среднее значение коэффициента доступности Операционного центра Платежной системы за календарный месяц, рассчитываемое по следующей формуле:

$$П4 = \left(\sum_{i=1}^{M} \left(1 - \frac{D_i}{T_i} \right) \Big/ M \right) \times 100\ \%,$$

где:

M - количество рабочих дней Платежной системы в месяце,

D_i - общая продолжительность всех приостановлений оказания операционных услуг Операционным центром Платежной системы 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 Платежной системы.

Показатель П4 рассчитывается ежемесячно в процентах с точностью до двух знаков после запятой (с округлением по математическому методу).

Значение показателя П4 по Платежной системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем Операционным центрам Платежной системы.

9.6.5. Показатель изменения частоты инцидентов (далее – «показатель П5»), характеризующий темп прироста частоты инцидентов.

Показатель П5 рассчитывается по Платежной системе в целом и для каждого Оператора УПИ 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:

$$П5 = \left(\frac{\sum_{i=1}^{M} КИ_i \Big/ M}{\sum_{i=1}^{N} КИ_i \Big/ N} - 1 \right) \times 100\%,$$

где:

$КИ_i$ - количество инцидентов в течение 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 календарных 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.

9.6.6. В Платежной системе установлены следующие пороговые уровни показателей БФПС:

- пороговый уровень показателя П1 - не более 6 часов для каждого из Операторов УПИ Платежной системы;
- пороговый уровень показателя П2 должен быть не менее 12 часов для каждого из Операторов УПИ Платежной системы;
- пороговый уровень показателя П3 должен быть не менее 98,0% для Операционного, Платежного клирингового центров Платежной системы (в том числе выполняющего функции ЦПКК), и не менее 99,0% для Расчетного центра Платежной системы;
- пороговый уровень показателя П4 должен быть не менее 96,0%;
- пороговый уровень показателя П5 должен быть не более 1250,0%.

9.6.7. Оператор Системы устанавливает и пересматривает с использованием результатов оценки рисков в Платежной системе пороговые уровни показателей БФПС.

9.6.8. Оператор Системы 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 и при оценке влияния инцидентов на БФПС.

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

9.6.10. Оценка влияния произошедшего в Платежной системе инцидента на БФПС осуществляется в соответствии с требованиями пп. 2.3.5 и 2.3.6 Положения Банка России №607-П.

9.6.11. В Платежной системе определены следующие критерии отнесения событий, реализовавшихся при оказании УПИ в Платежной системе, к событиям приостановления оказания УПИ:

а) для Операционного центра:

- невозможность приема Операционным центром ни одного Распоряжения Клиента/Участника Платежной системы в течение последовательных 6 часов и более;
- невозможность передачи ни одного обработанного Распоряжения Участников в Платежный клиринговый центр в течение последовательных 6 часов и более;

б) для Платежного клирингового центра:

- невозможность осуществления проверки Лимита Участника в отношении всех Участников в течение последовательных 6 часов и более при надлежащем выполнении своих обязательств Операционным центром и Расчетным центром;
- невозможность формирования платежно-клиринговой позиции для всех Участников и Отчета по операциям ЦПКК за предыдущий день в течение последовательных 6 часов и более после истечения сроков, определенных Временным регламентом Платежной системы для данного вида регламентных работ (п. 7.3.5 Правил);
- невозможность передачи Платежным клиринговым центром Отчетов Участникам и Отчета по операциям ЦПКК, и(или) Реестра Расчетному центру в течение последовательных 6 часов и более по истечении времени, предусмотренного Временным регламентом для данного вида регламентных работ (п. 7.3.5 Правил);

в) для Расчетного центра:

- невозможность информирования Платежного клирингового центра о проведении расчетов между Участниками и по Счетам ЦПКК более 6 (шести) часов по истечении времени, предусмотренного Временным регламентом для данного вида регламентных работ (п. 7.3.5 Правил), сопровождающееся отсутствием информационного обмена с Расчетным центром по вине Расчетного центра;
- невозможность информирования Платежного клирингового центра об остатках денежных средств на Счетах Участников, открытых в Расчетном центре для осуществления расчетов в рамках Платежной системы, и на Счете ЦПКК (в случае его открытия в Расчетном центре) в течение последовательных 6 часов и более в течение операционного дня Расчетного центра.

9.6.12. К событиям приостановления не относится приостановление оказания УПИ в связи проведением технологических и(или) регламентных работ в случае, если Оператор УПИ заранее уведомил об этом Оператора и Участников в соответствии с Правилами и(или) иными документами Оператора и(или) привлеченных Операторов УПИ.

9.6.13. Оператор устанавливает период времени, в течение которого должно быть восстановлено оказание УПИ в случае приостановления их оказания: не более 6 часов с момента приостановления оказания УПИ.

9.6.14. Оператор устанавливает период времени, в течение которого должно быть восстановлено оказание УПИ, соответствующее требованиям к оказанию услуг, в случае нарушения указанных требований: не более 24 часов с момента обнаружения Оператором Системы нарушения требований к оказанию УПИ.

9.6.15. Оператор обеспечивает оказание УПИ при возникновении инцидентов, а также организует в течение установленных в пункте 9.6.13 и пункте 9.6.14 Правил периодов времени восстановление оказания УПИ Операторами УПИ в случае приостановления их оказания и восстановление оказания УПИ, соответствующего требованиям к оказанию услуг, в случае нарушения указанных требований, установленных Правилами и действующим законодательством РФ.

9.6.16. Оператор, Операторы УПИ обязаны иметь планы обеспечения непрерывности деятельности и восстановления деятельности (далее – План ОНиВД), а также обеспечить их тестирование и пересмотр не реже одного раза в два года. План ОНиВД должен соответствовать требованиям и рекомендациям Банка России в части обеспечения и восстановления непрерывности деятельности.

9.7. Порядок обеспечения бесперебойности функционирования Платежной системы

9.7.1. В целях обеспечения БФПС Оператором устанавливается порядок осуществления Субъектами скоординированной деятельности, направленной на достижение, подтверждение и поддержание допустимого уровня рисков нарушения БФПС, под которыми понимаются присущие функционированию Платежной системы типичные возможности неоказания, ненадлежащего оказания услуг Платежной системы Участникам Платежной системы вследствие наступления неблагоприятных событий, связанных с внутренними и внешними факторами функционирования Платежной системы (далее – «факторы риска нарушения БФПС»).

9.7.2. Требования к содержанию деятельности по обеспечению БФПС, осуществляемой Оператором, Операторами УПИ и Участниками, должны включать в себя:

- требования к детализации допустимого уровня рисков нарушения БФПС в разрезе категорий Субъектов по видам их деятельности или участия в Платежной системе;
- порядок разработки, применения и оценки эффективности методик анализа рисков в Платежной системе, требования к оформлению и проверке результатов анализа;
- порядок оценки качества и надежности функционирования информационных систем, операционных и технологических средств, применяемых Операторами УПИ;

- порядок выбора и реализации мероприятий и способов достижения и поддержания допустимого уровня рисков нарушения БФПС, порядок оценки их эффективности и совершенствования;
- требования к мониторингу рисков нарушения БФПС;
- требования к планам обеспечения непрерывности деятельности и восстановления деятельности Операторов УПИ.

9.7.3. Порядок информационного взаимодействия Субъектов и документационного обеспечения их деятельности по обеспечению БФПС включает:

- перечень документов, используемых Субъектами при осуществлении деятельности по обеспечению БФПС, и порядок их составления;
- порядок информирования Оператора о событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, результатах расследования указанных событий, анализа их причин и последствий;
- порядок информирования Оператора о неисполнении или ненадлежащем исполнении обязательств Участников;
- порядок сбора, документирования и статистической обработки первичной информации о функционировании Платежной системы.

9.7.4. Оператор организует сбор и обработку сведений, в том числе от привлеченных Операторов УПИ, используемых для расчета показателей БФПС, указанных в пп. 9.6.1-9.6.5 Правил (далее – «сведения по Платежной системе»).

Первичная информация о функционировании Платежной системы включает в себя:

- информацию о времени приема к исполнению, исполнения Распоряжений Участников об осуществлении перевода денежных средств, количестве и суммах указанных Распоряжений (в том числе по каждому Участнику, являющемуся Отправителем или Получателем денежных средств);
- информацию о размерах клиринговых позиций и остатках денежных средств на Счетах Участников, открытых в Расчетном центре, а также информацию об остатках на Счетах ЦПКК;
- иную информацию о функционировании Платежной системы, предусмотренную настоящими Правилами.

9.7.5. Субъекты Платежной системы организуют деятельность по реализации порядка обеспечения БФПС в рамках внутренних систем управления рисками своей деятельности.

9.7.6. Деятельность Оператора по обеспечению БФПС включает:

- осуществление координации деятельности Субъектов по обеспечению БФПС;
- разработку внутренних документов в части реализации деятельности системы управления рисками и БФПС;
- установление допустимого уровня рисков нарушения БФПС не реже одного раза в квартал;
- определение продолжительности периода времени, в течение которого надлежащее функционирование Платежной системы должно быть восстановлено в случае его нарушения, в том числе в случае приостановления (прекращения) оказания услуг платежной инфраструктуры;
- мониторинг рисков нарушения БФПС в целях выявления текущих изменений присущего уровня риска нарушения БФПС;
- анализ рисков нарушения БФПС (выявление факторов риска нарушения БФПС, определение степени и характера влияния указанных факторов на БФПС, оценку присущего уровня рисков нарушения БФПС и подтверждение соответствия присущего уровня рисков нарушения БФПС установленному допустимому уровню рисков);

- принятие мер, необходимых для достижения или поддержания допустимого уровня рисков нарушения БФПС;
- проведение расследований событий, вызвавших операционные сбои, анализ их причин и последствий;
- принятие мер по устранению или минимизации рисков нарушения БФПС. К Субъектам применяются санкции, предусмотренные заключенными с ними договорами, в случае несоответствия установленному уровню БФПС;
- мероприятия, направленные на управление непрерывностью функционирования Платежной системы в случае возникновения инцидентов, связанных с приостановлением оказания услуг платежной инфраструктуры или нарушению установленных уровней оказания УПИ, предусмотренных пунктом 9.7.19 Правил;
- обеспечение восстановления надлежащего функционирования Платежной системы в случае его нарушения, в том числе восстановление оказания услуг платежной инфраструктуры;
- выявление в Платежной системе организаций, предоставляющих ее 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 Клиентам. Привлечение указанных организаций в качестве Операторов УПИ в соответствии с функциональными обязанностями Оператора;
- проведение оценки качества функционирования операционных и технологических средств и информационных систем не реже 1 (одного) раза в год, а также принятие решения об изменении операционных, технологических средств и процедур по результатам проведения такой оценки;
- проведение оценки рисков, присущих видам деятельности Оператора Платежной системы, для обеспечения непрерывности деятельности Платежной системы;
- оценка финансовой устойчивости Участников и Операторов УПИ (анализ финансовой отчетности и других документов, предоставляемых Участниками/Операторами УПИ);
- координация деятельности и осуществление информационного взаимодействия Субъектов в целях управления рисками нарушения БФПС.

9.7.7. Деятельность Операторов УПИ по обеспечению БФПС осуществляется в соответствии с функциональными обязанностями Субъекта в рамках Платежной системы и включает:

- организацию и осуществление деятельности по обеспечению бесперебойности оказания услуг Участникам в соответствии с функциональными обязанностями Субъекта в рамках системы управления рисками Платежной системы;
- разработку внутренних документов в части реализации своей деятельности в Системе по управлению рисками и обеспечению БФПС;
- разработку плана и порядка действий для обеспечения непрерывности оказания операционных услуг, платежных клиринговых услуг и расчетных услуг;
- установку допустимых технологических перерывов в оказании услуг платежной инфраструктуры в целях сохранения качества функционирования операционных и технологических средств. Общая продолжительность технологических перерывов не может превышать 48 (Сорок восемь) часов в течение каждого года работы;
- сбор и обработку первичной информации о времени поступления в Платежную систему Распоряжений Участников, 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;

- предоставление по запросу Оператора первичной информации о функционировании Платежной системы;
- сбор и обработку информации о событиях, вызвавших операционные сбои, об их причинах и последствиях, а также в случае возникновения или реализации угрозы неисполнения или ненадлежащего исполнения Участниками принятых на себя обязательств;
- ежемесячное предоставление Оператору Операторами УПИ сводной информации обо всех выявленных за отчетный месяц инцидентах в порядке, предусмотренном п. 9.10.7 Правил.
- организацию и осуществление деятельности по обеспечению бесперебойности оказания услуг Участникам в соответствии с принятыми на себя обязательствами и требованиями порядка обеспечения БФПС;
- мониторинг рисков нарушения БФПС;
- регулярную оценку качества и надежности функционирования применяемых информационных систем, работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Операторами УПИ, Участниками Платежной системы, их совершенствования;
- обеспечение собственной финансовой устойчивости (при выполнении функций Расчетного центра и(или) ПКЦ, являющегося ЦПКК), а именно – поддержание ликвидности, соблюдения экономических нормативов, поддержания финансовых показателей в соответствии с требованиями Банка России, обеспечение достаточности денежных средств на Счетах ЦПКК в Расчетном центре.

9.7.8. Деятельность Участников по обеспечению БФПС включает:

- предоставление Оператору в электронном виде финансовых отчетов (баланс, расчет обязательных экономических нормативов, расчет собственных средств и отчет о прибылях и убытках, иные документы по требованию Оператора) на каждую отчетную дату (если указанная отчетность не публикуется на сайте Участника или Банка России в объеме, достаточном для Оператора);
- проведение оценки рисков Участника, присущих его виду деятельности в Системе, для обеспечения непрерывности деятельности, включая обеспечение собственной финансовой устойчивости, а именно – поддержание ликвидности, соблюдения экономических нормативов, поддержания финансовых показателей в соответствии с требованиями применимого законодательства, обеспечение достаточности денежных средств на Счете Участника в Расчетном центре;
- принятие мер по обеспечению соответствия требованиям Платежной системы и надлежащего исполнения принятых на себя обязательств;
- незамедлительное (не позднее следующего рабочего дня с момента обнаружения) информирование Оператора о случаях неоказания или ненадлежащего оказания услуг, предоставляемых в рамках Платежной системы, и событиях, вызвавших операционные сбои, а также событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, об их причинах и последствиях;
- мониторинг рисков нарушения БФПС;
- самостоятельное проведение оценки качества функционирования операционных и технологических средств, информационных систем, автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования не реже 1 (одного) раза в год, а также предоставление Оператору по его запросу результатов оценки (по форме акта о проведении Участником тестирования качества функционирования модуля(ей), связанного(ых) с взаимодействием с Платежной системой) по Согласованным каналам связи;

- осуществление контроля соблюдения требований законодательства, настоящих Правил, договоров и условий осуществления переводов денежных средств;
- соблюдение требований настоящих Правил и принятых, в связи с этим обязательств.

9.7.9. К мониторингу риска нарушения БФПС предъявляются следующие требования:

- мониторинг рисков нарушения БФПС должен осуществляться Субъектами на постоянной основе (ежедневно);
- анализ достигнутых результатов должен осуществляться не реже одного раза в месяц.

9.7.10. Мониторинг риска нарушения БФПС должен производиться по следующим направлениям:

- выполнение финансовых обязательств;
- доступность технических сервисов.

9.7.11. С целью организации работы по обеспечению БФПС Операторы УПИ должны разработать и использовать в работе документы, устанавливающие политику обеспечения непрерывности деятельности и план восстановления деятельности системы после сбоев (План ОНиВД).

Операторы УПИ должны включать в Планы ОНиВД мероприятия по переходу на резервный комплекс программных и (или) технических средств Оператора УПИ в случае приостановления оказания УПИ и (или) нарушения установленных уровней оказания УПИ, а также мероприятия, осуществляемые в случае неработоспособности систем и сервисов привлеченных поставщиков (провайдеров), предоставляющих услуги в сфере информационных технологий в целях оказания Оператором УПИ услуг платежной инфраструктуры, нарушение предоставления которых способно привести к приостановлению оказания УПИ.

К планам ОНиВД Операторов УПИ предъявляются следующие требования:

- План ОНиВД должен описывать действия различных категорий работников Субъекта Платежной системы в аварийных ситуациях по ликвидации их последствий и минимизации наносимого ущерба;
- План ОНиВД должен быть работоспособным вне зависимости от того, какая авария случилась;
- План ОНиВД должен устанавливать ответственных и их обязанности за выполнение работ по восстановлению работоспособности.

В случае, если Оператор УПИ является кредитной организацией, разработка, проверка (тестирование) и пересмотр Плана ОНиВД осуществляется в порядке, предусмотренном Положением Банка России от 16.12.2003 года № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах», с учетом требований, содержащихся в пп. 2.3.10 и 2.3.11 Положения Банка России №607-П.

9.7.12. В целях осуществления деятельности по обеспечению БФПС Субъектам Системы рекомендуется разработать следующие документы[1]:

- положение о службе информационной безопасности;
- политика управления доступом и регистрацией;
- политика защиты от вредоносного кода;
- политика использования сети Интернет;
- политика резервного копирования;
- порядок учета объектов информационной инфраструктуры;

[1] Наименование перечисленных документов Субъектов Системы может быть отличным от указанных формулировок, но сохранять смысловое содержание, указанное в их наименовании

– документ(-ы), предусматривающий(-ие) действия сотрудников в ходе нештатных ситуаций, порядок ликвидации последствий аварийной ситуации, порядок расследования причин возникновения аварийной ситуации.

9.7.13. При разработке документов по обеспечению БФПС Субъекты должны учитывать требования законодательства Российской Федерации в области защиты информации и соответствующие Положения Банка России.

9.7.14. Оператор Платежной системы разрабатывает, проверяет (тестирует) и пересматривает план действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности (План ОНиВД) Оператора Платежной системы, с периодичностью не реже одного раза в два года.

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

– при совмещении в Платежной системе функций Оператора и Операционного центра, и(или) Платежного клирингового центра разрабатывает мероприятия по переходу на резервный комплекс программных и(или) технических средств, а также мероприятия, осуществляемые в случае неработоспособности систем и сервисов привлеченных поставщиков (провайдеров), предоставляющих услуги в сфере информационных технологий в целях оказания Оператором УПИ услуг платежной инфраструктуры, нарушение предоставления которых способно привести к приостановлению оказания УПИ;

– при наличии в Платежной системе двух и более Операционных, и (или) Платежных клиринговых, и (или) Расчетных центров - мероприятия по обеспечению взаимозаменяемости Операторов УПИ;

– при наличии в Платежной системе одного привлеченного Операционного, и (или) Платежного клирингового, и (или) Расчетного центров – мероприятия по привлечению другого Оператора УПИ и по переходу Участников Платежной системы на обслуживание к вновь привлеченному Оператору УПИ в течение не более одного года в случаях: превышения Оператором УПИ времени восстановления оказания УПИ при приостановлении их оказания более двух раз в течение трех месяцев подряд или нарушения Правил Платежной системы, выразившегося в отказе Оператора УПИ в одностороннем порядке от оказания услуг Участнику (Участникам) Платежной системы, не связанного с приостановлением (прекращением) участия в Платежной системе в случаях, предусмотренных Правилами Платежной системы.

9.7.16. Оператор Платежной системы обеспечивает реализацию мероприятий, указанных в п. 9.7.15 Правил.

9.7.17. Оператор Платежной системы организовывает разработку и контролирует наличие Планов ОНиВД у Операторов УПИ (с учетом требований, установленных в п. 9.7.11 Правил), проведение ими проверки (тестирования) и пересмотра Планов ОНиВД с периодичностью не реже одного раза в два года.

9.7.18. Оператор Системы анализирует эффективность мероприятий по восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг, и использует полученные результаты при управлении рисками в Платежной системе.

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

– надлежащий уровень оказания УПИ, при котором обеспечивается Стандартный режим функционирования Платежной системы.

– ненадлежащий уровень оказания УПИ, при котором не обеспечивается Стандартный режим функционирования Платежной системы. Возможны два режима функционирования Системы при ненадлежащем уровне оказания УПИ: Разрешенный и Критический.

9.7.20. Оператор устанавливает следующие режимы функционирования Платежной системы:

– Стандартный режим – режим оказания УПИ, при котором ни один из показателей БФПС не превышает значений, установленных ниже для данного режима. Стандартный режим функционирования Платежной системы соответствует гарантированному уровню бесперебойности оказания операционных услуг.

– Разрешенный режим – режим оказания УПИ с нарушениями требований к оказанию услуг, но не приводящими к нарушению функционирования Платежной системы, при котором ни один из показателей БФПС не превышает пороговых значений, установленных в п. 9.6.6 Правил.

– Критический режим – режим оказания УПИ с нарушениями, влияющими на БФПС и приводящими к невозможности оказания услуг Платежной системой.

Таблица соответствия пороговых значений показателей БФПС и режимов функционирования Платежной системы

Показатель БФПС		**Соответствие пороговых значений показателей БФПС и режимов функционирования Платежной системы**		
		Критический	**Разрешенный**	**Стандартный**
П1	Показатель продолжительности восстановления оказания УПИ	более 6 часов	2 - 6 часов	менее 2 часов
П2	Показатель непрерывности оказания УПИ	менее 12 часов	12 - 13 часов	более 13 часов
П3.1	Показатель соблюдения регламента (для операционного центра)	менее 98,0%	от 98,0% до 99,8%	более 99,8%
П3.2	Показатель соблюдения регламента (для клирингового центра и ЦПКК)	менее 98,0%	от 98,0% до 99,8%	более 99,8%
П3.3	Показатель соблюдения регламента (для расчетного центра)	менее 99,0%	от 99,0 до 99,1%	более 99,1%
П4	Показатель доступности операционного центра	менее 96,0%	от 96% до 99,95%	более 99,95%
П5	Показатель изменения частоты инцидентов	более 1250%	от 900% до 1250%	менее 900%

9.7.21. Обеспечение гарантированного уровня оказания операционных услуг в Платежной системе осуществляется путем выполнения следующих мероприятий и процедур:

– установлением порядка обеспечения БФПС (разделы 9.6 - 9.7, 9.10, 9.11 Правил);

– определением порядка управления рисками в Платежной системе (разделы 9.1–9.4, 9.8 Правил, Приложения №8-12 к Правилам);

– определением пороговых уровней показателей БФПС (п. 9.6.6 Правил):

– обеспечением восстановления оказания операционных услуг в течение времени, указанного в пп. 9.6.13 и 9.6.14 Правил.

9.8. Требования к методикам анализа рисков в Платежной системе, включая профили рисков

9.8.1. Оператор проводит плановую оценку рисков в Платежной системе, а также внеплановые оценки рисков с использованием методик анализа рисков в Платежной системе, включая профили рисков, требования к которым определены в главе 3 Положения Банка России №607-П.

9.8.1.1. Оператор проводит внеплановую оценку всех рисков в Платежной системе при внесении изменений в один или несколько процессов, в рамках которых обеспечивается оказание УПИ (далее – «бизнес-процесс»), или в несколько бизнес-процессов. Проведение внеплановой оценки всех рисков в Платежной системе должно быть завершено не позднее 6 (шести) месяцев со дня внесения указанных изменений.

9.8.1.2. Оператор проводит внеплановую оценку отдельных рисков (отдельного риска) в Платежной системе:

а) при возникновении события, реализация которого привела к приостановлению (прекращению) оказания УПИ и описание которого в профиле риска не предусмотрено, либо негативные последствия от его реализации превышают негативные последствия, предусмотренные для этого события в профиле риска;

б) при установлении по результатам проводимого Оператором мониторинга рисков факта приближения фактического уровня риска к уровню допустимого риска, при котором восстановление оказания УПИ, соответствующих требованиям к оказанию услуг, включая восстановление оказания УПИ в случае приостановления их оказания, осуществляется в течение периодов времени, установленных Оператором, и предполагаемый ущерб от которого Оператор готов принять без применения способов управления рисками в Платежной системе;

в) при выявлении значимого риска в Платежной системе, для которого уровень присущего риска до применения способов управления рисками в Платежной системе может превысить или превысил уровень допустимого риска.

Проведение внеплановой оценки отдельных рисков (отдельного риска) в Платежной системе должно быть завершено не позднее истечения 4 (четырёх) месяцев со дня возникновения событий, предусмотренных чч. а) и б) пп. 9.8.1.2 Правил, либо со дня выявления значимого риска в Платежной системе, указанного в ч. в) пп. 9.8.1.2 Правил.

9.8.1.3. Плановая оценка всех рисков в Платежной системе проводится Оператором не реже одного раза в 3 (три) года с учетом сведений о событиях, которые произошли в Платежной системе со дня завершения предыдущей плановой или внеплановой оценки всех рисков в Платежной системе и привели к приостановлению (прекращению) оказанию УПИ.

9.8.2. Оператор в целях управления рисками в Платежной системе разрабатывает методики анализа и оценки рисков в Платежной системе, включая риск нарушения БФПС (Приложения №8 и №9 к Правилам).

9.8.3. Методики анализа рисков в Платежной системе обеспечивают:

– выполнение процедур выявления Оператором рисков в Платежной системе не реже 1 (одного) раза в год;

– проведение анализа рисков в Платежной системе;

– выявление событий, реализация которых может привести к возникновению инцидента (далее - риск-события), и определение для каждого из выявленных риск-событий уровня риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации;

- определение для каждого из выявленных рисков в Платежной системе уровня присущего риска до применения способов управления рисками в Платежной системе (далее - уровень присущего риска), а также уровня допустимого риска, указанного в ч. б) пп. 9.8.1.2 Правил;
- определение значимых рисков в Платежной системе, указанных в ч. в) пп. 9.8.1.2 Правил;
- определение для каждого из значимых для Платежной системы рисков, указанных в ч. в) пп. 9.8.1.2 Правил, уровня остаточного риска после применения способов управления рисками в Платежной системе.

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

- формирование и поддержание в актуальном состоянии перечней бизнес-процессов (Приложение №10 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, в том числе анализа программных и(или) технических средств Операторов УПИ, учитывая факт привлечения ими поставщиков (провайдеров), предоставляющих услуги в сфере информационных технологий в целях оказания Оператором УПИ 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 для каждого из выявленных рисков в Платежной системе уровня присущего риска до применения способов управления рисками в Платежной системе и установление уровня допустимого риска, указанного в ч. б) пп. 9.8.1.2 Правил;
- сопоставление уровня присущего риска до применения способов управления рисками в Платежной системе и уровня допустимого риска, указанного в ч. б) пп. 9.8.1.2 Правил, по каждому из выявленных рисков в Платежной системе для определения значимых рисков в Платежной системе, указанных в ч. в) пп. 9.8.1.2 Правил;
- применение способов управления рисками в Платежной системе для каждого из значимых рисков в Платежной системе, указанных в ч. в) пп. 9.8.1.2 Правил, и последующее определение для них уровня остаточного риска после применения способов управления рисками в Платежной системе;
- сопоставление уровня остаточного риска после применения способов управления рисками в Платежной системе и уровня допустимого риска, указанного в ч. б) пп. 9.8.1.2 Правил, для каждого из значимых рисков в Платежной системе, указанных в ч. в) пп. 9.8.1.2 Правил, 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 уровня остаточного риска после применения способов управления рисками в Платежной системе, его соответствия уровню допустимого риска, указанного в ч. б) п. 9.1.8.2 Правил;
- составление и пересмотр (актуализацию) профиля каждого из значимых рисков в Платежной системе, указанных в ч. в) пп. 9.8.1.2 Правил, включая профиль риска нарушения БФПС (предусмотрены Приложениями №11 и №12 к Правилам).

9.8.5. Профили рисков составляются по всем значимым рискам в Платежной системе, указанным в ч. в) пп. 9.8.1.2 Правил, в том числе по следующим рискам:

- по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие несоблюдения Субъектами Платежной системы требований законодательства Российской Федерации, Правил Платежной системы, договоров, заключенных между Субъектами

Платежной системы, документов Оператора Платежной системы и документов Операторов УПИ либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России, Правилах Платежной системы и договорах, заключенных между Субъектами Платежной системы, а также вследствие нахождения Операторов УПИ и Участников Платежной системы под юрисдикцией различных государств (правовой риск Платежной системы);

- по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие возникновения у Субъектов Платежной системы сбоев, отказов и аварий в работе информационных и технологических систем, недостатков в организации и выполнении технологических и управленческих процессов, ошибок или противоправных действий персонала Субъектов Платежной системы либо вследствие воздействия событий, причины возникновения которых не связаны с деятельностью Субъектов Платежной системы, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц (операционный риск Платежной системы).

  В состав операционного риска включается также Риск ИБ, источниками реализации которых 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 операторами по переводу денежных средств, являющихся Участниками, и Операторами УПИ.

  В состав операционного риска Платежной системы включается также риск взаимодействия с привлеченными поставщиками (провайдерами), предоставляющими услуги в сфере информационных технологий в целях оказания Оператором УПИ услуг платежной инфраструктуры, в том числе обусловленный вероятностью невыполнения поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг;

- по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, ЦПКК или Расчетным центром Платежной системы вследствие невыполнения Участниками Платежной системы договорных обязательств перед указанными организациями в установленный срок или в будущем (кредитный риск Платежной системы);

- по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие отсутствия у ЦПКК и (или) у Участников Платежной системы денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами Платежной системы (риск ликвидности Платежной системы);

- по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие ухудшения финансового состояния Оператора Платежной системы и (или) Операторов УПИ, не связанного с реализацией кредитного риска Платежной системы и риска ликвидности Платежной системы (общий коммерческий риск Платежной системы).

9.8.6. Профиль каждого из значимых рисков в Платежной системе, указанных в ч. в) пп. 9.8.1.2 Правил, должен содержать:

- описание риск-событий, выявленных с применением не менее чем одного метода из числа предусмотренных Стандартом. Риск-события отражаются в профиле каждого из значимых рисков в Платежной системе, указанных в ч. в) пп. 9.8.1.2 Правил;
- описание причины возникновения каждого из риск-событий;
- описание бизнес-процессов, 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 до применения способов управления рисками в Платежной системе;
- уровень допустимого риска, указанный в указанных в ч. б) пп. 9.8.1.2 Правил;
- уровень остаточного риска после применения способов управления рисками в Платежной системе;
- перечень способов управления рисками в Платежной системе.

Профиль риска нарушения БФПС составляется как сводный профиль в отношении всех значимых рисков в Платежной системе, указанных в ч. в) пп. 9.8.1.2 Правил (Приложение №12 к Правилам).

9.8.7. Оператор пересматривает (актуализирует) профили рисков по результатам плановой или внеплановой оценки всех рисков в Платежной системе, а также внеплановой оценки отдельных рисков (отдельного риска) в Платежной системе.

9.8.8. Оператор должен хранить сведения, содержащиеся в профилях рисков, не менее пяти лет со дня составления и пересмотра (актуализации) профилей рисков.

9.9. Порядок обмена информацией, необходимой для управления рисками

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

9.9.2. Обмен информацией, необходимой для управления рисками, может осуществляться посредством использования Согласованных каналов связи, через доверенных операторов электронного документооборота, и/или в рамках ЭДО, предусмотренного настоящими Правилами.

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

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

9.9.5. Оператор обязуется предоставлять Участникам, Операторам УПИ информацию, требуемую в целях управления рисками в Платежной системе, как по собственной инициативе, так и по запросу последних.

9.10. Порядок информационного взаимодействия Субъектов Платежной системы в спорных, чрезвычайных и нестандартных ситуациях, включая случаи системных сбоев

9.10.1. С целью обеспечения БФПС Оператор Системы, Операторы УПИ, и Участники осуществляют информационное взаимодействие. Обмен информацией осуществляется способами, аналогичными указанным для обмена информацией, необходимой для управления рисками, и предусмотренным п. 9.9.2 Правил.

9.10.2. Оператор определяет порядок информационного взаимодействия Субъектов Платежной системы по обеспечению БФПС, установленный в пп. 9.10.3 - 9.10.8 Правил.

9.10.3. Участники и Операторы УПИ обязаны незамедлительно (не позднее следующего рабочего дня с момента обнаружения) доводить до Оператора информацию о следующих событиях:

а) о возникновении в процессе работы в Платежной системе нарушений и неисправностей либо об обстоятельствах, которые препятствуют исполнению операций, платежного клиринга или расчетов, повлекших за собой значительное нарушение допустимого уровня риска (включая случаи системных сбоев);

б) о наступлении спорных или чрезвычайных ситуаций;

в) о случаях или попытках осуществления переводов денежных средств без добровольного согласия клиента. Информирование Оператора по данному основанию осуществляется в порядке, предусмотренном разделом 10.6 Правил.

9.10.4. Информирование Оператора осуществляется по форме Приложения №7 к Правилам либо в иной форме, содержащей следующие сведения:

- время и дата возникновения инцидента (в случае невозможности установить время возникновения инцидента, указывается время его выявления);
- краткое описание инцидента (характеристика произошедшего инцидента и его последствия);
- наименование одного или нескольких бизнес-процессов, в ходе которых произошел инцидент;
- наименование одного или нескольких бизнес-процессов, на которые инцидент оказал влияние;
- мероприятия по устранению неблагоприятных последствий инцидента с указанием планируемой и фактической продолжительности проведения данных мероприятий (информация предоставляется после такого устранения);
- неблагоприятные последствия инцидента, в том числе: сумма денежных средств, уплаченных Оператором и (или) взысканных с Оператора; сумма денежных средств, уплаченных Оператором (Операторами) УПИ и (или) взысканных с Оператора (Операторов) УПИ; количество и сумма неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных Распоряжений Участников, на исполнение которых оказал влияние инцидент; продолжительность приостановления оказания УПИ.

9.10.5. Операторы УПИ, дополнительно к сведениям, предоставляемым согласно пункта 9.10.4 Правил, оперативно информируют Оператора Платежной системы о:

- наличии (отсутствии) факта приостановления оказания УПИ;
- времени и дате восстановления оказания УПИ в случае их приостановления;
- дате восстановления оказания УПИ, соответствующего требованиям, предъявляемым Оператором Системы к оказанию УПИ.

9.10.6. Оператор Системы незамедлительно с момента получения от Субъекта уведомления о наступлении инцидента совместно с соответствующими Субъектами Системы определяют план дальнейших действий индивидуально по каждому наступившему инциденту в целях устранения возникших операционных сбоев, в том числе их последствий, и предотвращения наступления новых.

9.10.7. Операторы УПИ ежемесячно (не позднее 5 (пяти) рабочих дней месяца, следующего за отчетным) предоставляют Оператору сводную информацию обо всех выявленных инцидентах с указанием количества инцидентов за отчетный месяц, дат их возникновения/выявления и значений показателей БФПС, а также дополнительную информацию об инцидентах по усмотрению Оператора УПИ. При отсутствии инцидентов в отчетном месяце Операторы УПИ в тот же срок направляют Оператору ПС отчет, содержащий нулевые данные.

9.10.8. Оператор Системы информирует о случаях и причинах приостановления (прекращения) оказания УПИ:

- Банк России (Департамент национальной платежной системы) посредством направления сообщения в течение двух рабочих дней со дня приостановления (прекращения) оказания УПИ; при этом Оператор Системы в день приостановления (прекращения) оказания УПИ незамедлительно направляет в Департамент национальной платежной системы Банка России уведомление о приостановлении (прекращении) оказания УПИ;
- Участников, Операторов УПИ в день такого приостановления (прекращения) любым из указанных ниже способов:
  - размещение информации на официальном сайте Оператора в сети Интернет;
  - направление уведомления по Согласованным каналам связи.

9.10.9. Оператор осуществляет сбор, систематизацию, накопление информации о возникновении аварийных ситуаций, а также проводит анализ причин нарушений функционирования операционных и технологических средств, устройств, информационных систем, выработку и реализацию мер по их устранению и недопущению.

9.10.10. Субъекты не вправе необоснованно отказать Оператору в предоставлении запрашиваемой информации, предусмотренной настоящим разделом. В случае если запрашиваемая информация содержит сведения, составляющие коммерческую или иную охраняемую законом тайну Субъекта, Оператор обязуется обеспечить сохранение такой информации в соответствии с требованиями законодательства Российской Федерации.

9.10.11. Оператор Системы обеспечивает хранение сведений по Платежной системе и сведений об инцидентах не менее 5 (пяти) лет с даты получения указанных сведений.

9.11. Контроль за соблюдением Субъектами Платежной системы порядка обеспечения БФПС

9.11.1. Оператор Платежной системы проверяет соблюдение Операторами УПИ и Участниками Платежной системы порядка обеспечения БФПС, установленного настоящими Правилами.

9.11.2. Для контроля за соблюдением Операторами УПИ и Участниками порядка обеспечения БФПС Оператор вправе запрашивать у Субъектов любую информацию, необходимую для обеспечения порядка БФПС. Субъекты обязаны предоставлять Оператору запрашиваемую информацию в срок, установленный в запросе Оператора.

9.11.3. Оператор контролирует соответствие документов Операторов УПИ и Участников порядку обеспечения БФПС и при выявлении несоответствия направляет рекомендации по устранению выявленных несоответствий.

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

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

9.11.5. Оператор устанавливает ответственность за неисполнение порядка обеспечения БФПС для Операторов УПИ и Участников в Правилах Платежной системы, в том числе в договорах с ними.

9.11.6. Действия Оператора при выявлении нарушения порядка обеспечения БФПС предусмотрены разделом 13 Правил.

9.12. Порядок изменения операционных и технологических средств и процедур

9.12.1. Решение о необходимости изменения операционных и технологических средств и процедур принимает Оператор.

9.12.2. Основанием для изменения операционных и технологических средств и процедур являются:

- включение новых типов операций по переводам денежных средств или внесение существенных изменений в действующие операции;
- замена или модернизация операционных и технологических средств, направленных на повышение качества оказания услуг по переводу денежных средств;
- внесение изменений в функционирование системы управления рисками;
- изменение действующего законодательства Российской Федерации.

9.12.3. Если изменение операционных и технологических средств и процедур требует внесения изменений в настоящие Правила, Оператор вносит соответствующие изменения в порядке, предусмотренном настоящими Правилами.

9.12.4. Если изменение операционных и технологических средств и процедур не требует внесения изменений в настоящие Правила, Оператор направляет Участникам соответствующее уведомление с описанием изменений не позднее, чем за 15 (пятнадцать) календарных дней до даты вступления в силу соответствующих изменений.

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

9.13.1. Оператор осуществляет оценку качества функционирования информационных систем, операционных и технологических средств и процедур Платежной системы с привлечением независимой организации.

9.13.2. Оценка качества функционирования информационных систем, операционных и технологических средств с привлечением независимой организации включает в себя следующие мероприятия, осуществляемые Оператором:

- принятие решения о привлечении независимой организации;
- выбор независимой организации;
- заключение договора с независимой организацией;
- предоставление независимой организации информации, необходимой для проведения оценки;
- выполнение независимой организацией работ по оценке качества и надёжности функционирования информационных систем, операционных и технологических средств;
- получение от независимой организации отчёта с результатами оценки и с рекомендациями по совершенствованию информационных систем, операционных и технологических средств.

9.13.3. На основании результатов оценки качества функционирования операционных и технологических средств и информационных систем Платежной системы независимой организацией и рекомендаций по совершенствованию Оператор вправе вносить изменения в функционирование операционных и технологических средств и процедур Платежной системы в порядке, предусмотренном настоящими Правилами.

9.13.4. Участники и Операторы УПИ самостоятельно и за свой счет по своему усмотрению либо в силу требований применимого законодательства проводят оценку качества функционирования операционных и технологических средств и информационных систем, применяемых на стороне Участников и Операторов УПИ. Оператор вправе запросить информацию о факте проведения указанной оценке и(или) о ее результатах.

10. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ПЛАТЕЖНОЙ СИСТЕМЕ МАРЛИН

10.1. Общие требования к порядку обеспечения защиты информации

10.1.1. Защита информации при осуществлении переводов денежных средств в рамках Системы осуществляется всеми Субъектами Системы в соответствии с требованиями законодательства Российской Федерации[1] в области защиты информации, Постановлением Правительства Российской Федерации от 13 июня 2012 года №584 «Положение о защите информации в платежной системе» (далее – «Постановление Правительства Российской Федерации от 13 июня 2012 года №584»), Положением Банка России №821-П и настоящих Правил.

10.1.2. Защита информации обеспечивается путем реализации Субъектами Платежной системы правовых, организационных и технических мер, направленных:

- на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении информации;
- на соблюдение конфиденциальности, целостности, доступности и достоверности информации;
- на регламентацию, реализацию, контроль (мониторинг) технологии обработки защищаемой информации;
- на регистрацию результатов совершения действий, связанных с осуществлением доступа к защищаемой информации.

10.1.3. Субъекты Системы должны регистрировать результаты совершения следующих действий, связанных с осуществлением доступа к защищаемой информации:

- идентификации, аутентификации и авторизации клиентов операторов по переводу денежных средств при совершении действий в целях осуществления переводов денежных средств;
- приема электронных сообщений от клиентов операторов по переводу денежных средств;
- приема (передачи) электронных сообщений при взаимодействии Субъектов Системы при осуществлении переводов денежных средств, в том числе для удостоверения права клиентов операторов по переводу денежных средств распоряжаться денежными средствами и для учета результатов переводов денежных средств;
- реализации мер, направленных на проверку правильности формирования (подготовки) электронных сообщений (двойной контроль);
- осуществления доступа работников к защищаемой информации, выполняемого с использованием автоматизированных систем, программного обеспечения;
- осуществления действий клиентов операторов по переводу денежных средств с защищаемой информацией, выполняемых с использованием автоматизированных систем, программного обеспечения.

10.1.4. Требования к обеспечению защиты информации при осуществлении переводов денежных средств применяются для обеспечения защиты следующей информации, содержащейся в Платежной системе (далее - защищаемая информация):

- информации об остатках денежных средств на Счетах Участников;
- информации, содержащейся в электронных сообщениях, обмен которыми осуществляется при взаимодействии Субъектов Платежной системы;

[1] Здесь и далее – для иностранных Субъектов в соответствии с применимым законодательством.

- информации об осуществлении перевода денежных средств, содержащейся в Отчетах и(или) реестрах электронных сообщений, направляемых Субъектами Платежной системы;
- информации о совершенных переводах денежных средств, в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению Распоряжений Участников, а также в извещениях (подтверждениях), касающихся исполнения Распоряжений Участников;
- информации о платежных клиринговых позициях;
- информации, необходимой для удостоверения права Участников распоряжаться денежными средствами;
- информации, используемой для идентификации, аутентификации и авторизации Субъектов при осуществлении переводов денежных средств;
- ключевой информации средств криптографической защиты информации (далее - СКЗИ), используемая при осуществлении обмена электронными сообщениями между Субъектами Платежной системы;
- информации о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Участником или привлеченными ими лицами, Оператором УПИ, и используемых для осуществления переводов денежных средств (далее – «объекты информационной инфраструктуры»), а также информации о конфигурации, определяющей параметры работы технических средств защиты информации;
- 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.

10.1.5. Требования к обеспечению защиты информации при осуществлении переводов денежных средств предусматривают:

- защиту информации при назначении и распределении функциональных прав и обязанностей (далее – «ролей») лиц, связанных с осуществлением переводов денежных средств;
- разработку и реализацию систем защиты информации в информационных системах;
- определение порядка доступа к объектам инфраструктуры Платежной системы, обрабатывающим информацию;
- применение на объектах инфраструктуры лицензированного антивирусного программного обеспечения, своевременное его обновление, а также непрерывное его использование;
- обеспечение защиты информации при использовании информационно-телекоммуникационных сетей общего пользования;
- 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);
- создание и организацию функционирования подразделения, ответственного за организацию и контроль обеспечения защиты информации (далее - служба информационной безопасности) или назначение должностного лица (работника), ответственного за организацию защиты информации;
- повышение осведомленности работников Субъектов Платежной системы и Клиентов (далее - повышение осведомленности) в области обеспечения защиты информации;
- включение в должностные обязанности работников, участвующих в обработке информации, обязанностей по выполнению требований к защите информации;

- осуществление мероприятий, имеющих целью определение угроз безопасности информации и анализ уязвимости информационных систем;
- выявление инцидентов, связанных с нарушениями требований к обеспечению защиты информации и реагированию на них;
- определение и реализация порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- организация и проведение контроля и оценки выполнения требований к защите информации на собственных объектах информационной инфраструктуры не реже 1 раза в 2 года;
- обеспечение защиты информации при осуществлении переводов денежных средств с применением ЭСП;
- проведение анализа рисков нарушения требований к защите информации и управление такими рисками.

10.1.6. Оператор Системы устанавливает порядок обеспечения защиты информации в Системе, при определении которого Участники должны реализовать следующие мероприятия:

а) установить состав и пороговые значения показателей уровня Риска ИБ Участника Системы, с учетом указанных в Приложении №6 к Правилам, в состав которых входит количество инцидентов нарушения информационной безопасности и размер убытков от инцидентов Риска ИБ Участника;

б) реализовать механизмы, направленные на соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств. В рамках контроля реализации механизмов, направленных на соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств, Оператор Системы может запросить у операторов по переводу денежных средств, являющихся Участниками Системы, и Операторов УПИ информацию согласно Приложению №5 к Правилам;

в) операторы по переводу денежных средств, являющиеся Участниками Системы, и Операторы УПИ должны выстроить процессы выявления и идентификации Риска ИБ Участника Системы, исходя из источников их реализации и причин возникновения. При выполнении мероприятий по выявлению и идентификации Риска ИБ в отношении своих объектов информационной инфраструктуры Оператор устанавливает следующие требования к операторам по переводу денежных средств, являющимся Участниками Системы, и Операторам УПИ:

- определять потенциальные угрозы (риски) в отношении объектов информационной инфраструктуры, используемых Участниками и Операторами УПИ для работы в Платежной системе;
- в рамках СУР ИБ Участников и Операторов УПИ классифицировать Риски ИБ в отношении объектов информационной инфраструктуры, используемых ими для работы в Платежной системе;
- для выявления и идентификации Риска ИБ использовать способы, включающие в себя в том числе, но не ограничиваясь: анализ произошедших риск-событий, интервьюирование работников Субъекта, позволяющие установить Риски ИБ, оказывающие влияние на работу Субъекта в Платежной системе, анализ документации, полученной в результате внутреннего и внешнего аудита и других источников информации.

При проведении мероприятий по выявлению и идентификации Риска ИБ в отношении своих объектов информационной инфраструктуры, используемых при работе в ПС, Субъект должен руководствоваться положениями нормативных актов Банка России, внутренними документами, регламентирующими управление Риском ИБ, и требованиями Оператора;

г) операторы по переводу денежных средств, являющиеся Участниками Системы, и Операторы УПИ должны проводить оценку Рисков ИБ в Системе. В целях проведения оценки Риска ИБ Участника Системы Оператор устанавливает следующие требования к операторам по переводу денежных средств, являющимся Участниками Системы, и Операторам УПИ:

- проводить анализ и оценку внешних и внутренних факторов, влияющих на информационную безопасность объектов информационной инфраструктуры и бизнес-процессов, в которых участвует Участник при осуществлении операций в Платежной системе;
- идентифицировать Риски ИБ, которые могут возникнуть при работе в Платежной системе;
- разработать и поддерживать в актуальном состоянии классификаторы Рисков ИБ, риск-событий, причин возникновения риск-событий. При формировании перечня риск-событий учитывать внутренние документы Субъекта, регламентирующие порядок защиты информации при осуществлении переводов денежных средств, результаты оценки соответствия требованиям безопасности, известные уязвимости на объектах информационной инфраструктуры, используемых для выполнения функциональных обязанностей в Платежной системе;
- определить уровни присущего Риска ИБ и установить уровень допустимого Риска ИБ, выделить значимые Риски ИБ, определить вероятность реализации Риска ИБ, идентифицированного соответствующим Субъектом, при работе в Платежной системе;
- определить способы управления Риском ИБ и, по необходимости, актуализировать их;
- вести мониторинг Рисков ИБ, в том числе уровней остаточных Рисков ИБ, и контролировать их соответствие допустимым уровням Рисков ИБ.

Наряду с требованиями Оператора, указанными в настоящем подпункте, оператор по переводу денежных средств, являющийся Участником, и Операторы УПИ должны:

- вести базу инцидентов защиты информации;
- своевременно информировать Оператора о реализации Риска ИБ у Субъекта или о потенциальной угрозе реализации риска ИБ;
- предпринимать действия, направленные на минимизацию возможных негативных последствий от реализации у Субъекта Риска ИБ при работе в Платежной системе;
- обеспечивать выполнение требований по защите информации при осуществлении переводов денежных средств.

д) операторы по переводу денежных средств, являющиеся Участниками Системы, и Операторы УПИ должны внедрить процессы реагирования на инциденты защиты информации и восстановления штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации, которые должны обеспечивать выполнение условий Положения по управлению инцидентами защиты информации при осуществлении переводов денежных средств в Платежной системе МАРЛИН (Приложение №4 к Правилам);

е) операторы по переводу денежных средств, являющиеся Участниками Системы, и Операторы УПИ должны обеспечить взаимодействие при обмене информацией об инцидентах защиты информации согласно Приложению №4 к Правилам;

ж) операторы по переводу денежных средств, являющиеся Участниками Системы, и Операторы УПИ должны реализовать мероприятия по противодействию осуществлению переводов денежных средств без добровольного согласия клиента, определенные Указанием Банка России от 19 августа 2024 г. №6828-У «О порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без добровольного согласия клиента, форме и порядке получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, порядке запроса и получения Банком России у них информации о переводах денежных средств, связанных с переводами денежных средств без добровольного согласия клиента, в отношении которых от федерального органа исполнительной власти в сфере внутренних дел получены сведения о совершенных противоправных действиях в соответствии с частью 8 статьи 27 Федерального закона от 27 июня 2011 года №161-ФЗ «О

национальной платежной системе», а также о порядке реализации ими мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента» (далее – «Указание Банка России №6828-У»);

и) устранять причины, способствовавшие установлению Оператором Системы ограничений по параметрам операций по осуществлению переводов денежных средств в случае превышения пороговых значений показателей уровня Риска ИБ, установленных Приложением №6 к Правилам.

10.1.7. Оператор Системы в Приложении №6 к Правилам устанавливает состав и пороговые значения показателей Риска ИБ Участника Системы, где также отражены типы ограничений по параметрам операций по осуществлению переводов денежных средств и условия снятия таких ограничений.

В рамках мероприятий по контролю за соблюдением пороговых значений показателей уровня Риска ИБ Участника Системы Оператор анализирует информацию об инцидентах защиты информации, полученную от Субъектов в порядке, предусмотренном пп. 9.10.3-9.10.5, 9.10.7 Правил и Приложением №4.

В случае выявления факта превышения пороговых значений показателей уровня Риска ИБ Участника Системы Оператор применяет к операторам по переводу денежных средств, являющихся Участниками Системы, и к Операторам УПИ ограничения по параметрам операций по осуществлению переводов денежных средств, указанные в Приложении №6 к Правилам. В случаях, предусмотренных Приложением №6 Правил, Оператор снимает ранее примененные ограничения.

10.1.8. К инцидентам, связанным с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, относят события, которые привели или могут привести к осуществлению переводов денежных средств без добровольного 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 (далее - перечень типов инцидентов).

10.1.9. Выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств обеспечивается путем:

- выбора организационных мер защиты информации;
- выбора технических средств защиты информации;
- применения объектов информационной инфраструктуры, обладающих функциональными и конструктивными особенностями, связанными с обеспечением защиты информации при осуществлении переводов денежных средств и реализации контроля за их функционированием.

10.1.10.Оператор вносит изменения в Правила в части, касающейся требований к защите информации в следующих случаях:

- при изменениях в законодательных актах Российской Федерации;
- при изменениях в нормативных актах Банка России, регулирующих отношения в национальной платежной системе;
- при совершенствовании Системы и (или) порядка защиты информации в Системе;
- при изменении порядка оказания услуг.

10.2. Порядок обеспечения защиты информации

10.2.1. Субъекты Платежной системы обязаны обеспечивать защиту информации при осуществлении переводов денежных средств и использовании ЭСП, при обмене электронными сообщениями, при хранении и обработке информации, связанной с их деятельностью в Системе, в соответствии с

требованиями, установленными Банком России, согласованными с федеральными органами исполнительной власти, и настоящих Правил.

10.2.2. Субъекты Системы должны обеспечивать безопасность технологического процесса обработки, передачи и хранения защищаемой информации, согласованное применение технологических и организационных мер, технических и программных средств защиты информации на всех этапах подготовки, обработки, передачи и хранения защищаемой информации.

10.2.3. Субъекты Платежной системы обязаны 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.

10.2.4. Каждый Субъект самостоятельно определяет порядок обеспечения защиты информации в соответствии с законодательством Российской Федерации и настоящими Правилами в соответствии со своим статусом и в рамках своих функциональных обязанностей в Платежной системе.

10.2.5. Субъекты Платежной системы обязаны подготовить и утвердить внутренние документы, устанавливающие требования к защите информации при осуществлении переводов денежных средств и (или) операций с использованием ЭСП, включая способы и методы обеспечения указанных требований.

10.2.6. Субъекты Платежной системы самостоятельно с учетом требований Положения Банка России №821-П определяют порядок проведения 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, а также программного обеспечения, эксплуатируемого на участках, используемых для приема электронных документов, связанных с осуществлением переводов денежных средств, к исполнению в автоматизированных системах и приложениях с использованием сети «Интернет».

10.2.7. Для проведения работ по защите информации Субъектами 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.

10.2.8. Контроль соблюдения требований к защите информации осуществляется Субъектами самостоятельно.

10.2.9. Субъекты Системы обязаны сформировать службы информационной безопасности или назначить ответственное лицо за организацию защиты информации, а также определить во внутренних документах цели и задачи деятельности этой службы или ответственных лиц.

10.2.10.Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется следующими полномочиями:

- осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации;
- определять требования к техническим средствам защиты информации и организационным мерам защиты информации;
- контролировать выполнение работниками требований к обеспечению защиты информации;
- участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации;
- участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации, применяемых при восстановлении предоставления услуг Системы после сбоев и отказов в работе объектов информационной инфраструктуры.

10.2.11.Структурное подразделение (ответственное лицо) по защите информации и структурное подразделение по информатизации (автоматизации) не должны иметь общего куратора.

10.2.12.Субъект Платежной системы обеспечивает регистрацию работников, участвующих в обработке информации, обладающих правами:

- по осуществлению доступа к защищаемой информации;
- по управлению криптографическими ключами;
- по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг.

10.2.13.Запрещается выполнение одним лицом в один момент времени следующих ролей:

- связанных с созданием (модернизацией) объекта информационной инфраструктуры и эксплуатацией объекта информационной инфраструктуры;
- связанных с эксплуатацией объекта информационной инфраструктуры в части его использования по назначению и эксплуатацией объекта информационной инфраструктуры в части его технического обслуживания и ремонта.

10.2.14.Для защиты информации от воздействия вредоносного кода, приводящего к нарушению штатного функционирования средств вычислительной техники (далее – «вредоносный код») Субъекты Системы обеспечивают:

- использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры (использование антивирусного программного обеспечения), на средствах вычислительной техники, включая банкоматы и платежные терминалы, при наличии технической возможности;
- регулярное обновление версий антивирусного программного обеспечения и баз данных, используемых в их работе 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;
- формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода (указанное требование распространяется на операторов по переводу денежных средств, являющихся Субъектами Системы);
- использование антивирусного программного обеспечения различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления операций, а также на межсетевых экранах, задействованных в осуществлении операций, при наличии технической возможности;
- выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы, при наличии технической возможности;
- выполнение проверки на отсутствие вредоносного кода средств вычислительной техники, включая банкоматы и платежные терминалы, выполняемой после установки или изменения программного обеспечения, при наличии технической возможности.

10.2.15.В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Субъекты Системы:

- обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода;
- приостанавливают при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом;

- обеспечивают информирование Оператора. Оператор обеспечивает информирование Операторов УПИ и Участников.

10.2.16.При использовании информационно-телекоммуникационных сетей общего пользования для осуществления переводов денежных средств Субъекты обеспечивают:

- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации, передаваемой по информационно-телекоммуникационным сетям общего пользования;
- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры;
- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения;
- минимизацию негативных последствий, связанных с несвоевременностью осуществления переводов денежных средств, сбоями или отказами в работе объекта информационной инфраструктуры;
- фильтрацию сетевых пакетов при обмене информацией между информационно-телекоммуникационными сетями, в которых располагаются объекты информационной инфраструктуры, и информационно-телекоммуникационными сетями общего пользования с целью защиты от негативного внешнего воздействия.

10.2.17. Для обеспечения защиты информации при совершении операций, связанных с осуществлением переводов денежных средств, Субъекты Системы должны применять следующие технологические меры на соответствующих технологических участках:

- реализация механизма идентификации, аутентификации и авторизации клиентов операторов по переводу денежных средств при совершении ими действий в целях осуществления переводов денежных средств;
- реализация механизма двухфакторной аутентификации клиентов операторов по переводу денежных средств при совершении ими действий в целях осуществления переводов денежных средств;
- применение механизмов и (или) протоколов формирования и обмена электронными сообщениями, обеспечивающих защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации, в том числе аутентификацию входящих электронных сообщений;
- взаимная (двухсторонняя) аутентификация участников обмена средствами вычислительной техники Субъектов Системы;
- использование электронной подписи в соответствии с Федеральным законом от 6 апреля 2011 года №63-ФЗ «Об электронной подписи»;
- использование усиленной электронной подписи в целях обеспечения целостности электронных сообщений и подтверждения их составления уполномоченным на это лицом;
- получение подтверждения от Участника/Расчетного центра права клиента распоряжаться денежными средствами;
- проверка соответствия (сверка) результатов осуществления операций, связанных с переводом денежных средств, с информацией, содержащейся в электронных сообщениях;

- реализация мер, направленных на проверку правильности формирования (подготовки) электронных сообщений (двойной контроль);
- обеспечение хранения защищаемой информации, информации о событиях, подлежащих регистрации, информации об инцидентах защиты информации в течение пяти лет с даты формирования информации в неизменном виде;
- восстановление защищаемой информации в случае умышленного или случайного разрушения либо выхода из строя средств вычислительной техники.

10.2.18.Доступ к ПО Системы производится с использованием персонифицированных учетных записей. Пароли для учетных записей должны соответствовать внутренним требованиям Субъектов, при этом должно быть обеспечено:

- использование в пароле не менее 8 символов (должен в обязательном порядке содержать: заглавные и прописные буквы, цифры, спецсимволы);
- периодичность смены пароля не реже одного раза в 90 дней с запретом использования любого из 4-х предыдущих паролей;
- защита пароля при хранении и в процессе работы;
- в случае подозрения на компрометацию пароля учетной записи должна быть немедленно произведена внеплановая смена пароля;
- временная блокировка учетной записи пользователей после выполнения 10 неуспешных последовательных попыток аутентификации на период времени не менее 30 мин.

10.2.19. Субъектам Системы запрещается использовать неперсонифицированные учетные записи и административные учетные записи для создания переводов через ПО Системы. Пароли от административных учетных записей должны отличаться от пользовательских паролей, используемых для доступа к ПО Системы в целях осуществления операций по переводу денежных средств и соответствовать следующим требованиям:

- использование в пароле не менее 16 символов (должен в обязательном порядке содержать: заглавные и прописные буквы, цифры, спецсимволы);
- периодичность смены пароля не реже одного раза в 90 дней с запретом использования любого из 4-х предыдущих паролей;
- защита пароля при хранении и в процессе работы;
- в случае подозрения на компрометацию пароля учетной записи должна быть немедленно произведена внеплановая смена пароля;
- временная блокировка учетной записи пользователей после выполнения 10 неуспешных последовательных попыток аутентификации на период времени не менее 30 мин.

10.2.20. Субъекты обеспечивают повышение осведомленности работников в области обеспечения защиты информации:

- по порядку применения организационных мер защиты информации;
- по порядку использования технических средств защиты информации.

10.2.21.Участник обеспечивает доведение до Клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению, в том числе информации о:

- рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого Клиентом осуществлялся перевод денежных средств;

- рекомендуемых мерах по контролю конфигурации устройства, с использованием которого Клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода;
- появлении в сети "Интернет" ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых оператором по переводу денежных средств систем Интернет-банкинга, и (или) использующих зарегистрированные товарные знаки и наименование оператора по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения.

10.2.22.В целях выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагирования на них Субъекты обеспечивают:

- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- информирование службы информационной безопасности, в случае ее наличия, или ответственных лиц о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты.

10.2.23.Требования к порядку, форме и срокам информирования Оператора, Участников и Операторов УПИ, а также требования к порядку взаимодействия Субъектов в случае выявления в Платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, приведены в «Положении по управлению инцидентами, связанными с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе МАРЛИН» (Приложение №4).

10.2.24.Оператор обеспечивает учет и доступность для Участников и Операторов УПИ путем размещения в ЛК или направления по Согласованным каналам связи следующей информации:

- о выявленных в Платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- о способах реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

10.3. Использование средств криптографической защиты информации

10.3.1. Защита информации при осуществлении переводов денежных средств с использованием средств криптографической защиты информации (далее – «СКЗИ») осуществляется в следующем порядке.

10.3.2. Обеспечение защиты информации при осуществлении переводов денежных средств с помощью средств криптографической защиты информации (далее – «СКЗИ») осуществляется в соответствии с Федеральным законом от 6 апреля 2011 года №63-ФЗ «Об электронной подписи», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации, утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года №66 (далее – «Положение ПКЗ-2005»), и технической документацией на СКЗИ.

В случае если Субъекты Платежной системы применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты соответствия требования, установленным федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и соответствовать классу защиты не ниже КС1.

10.3.3. В случае применения СКЗИ Субъекты Платежной системы определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления переводов денежных средств;
- порядок эксплуатации СКЗИ;
- порядок восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе;
- порядок внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ;
- порядок снятия с эксплуатации СКЗИ;
- порядок управления ключевой системой;
- порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей.

10.3.4. Оператор Платежной системы определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации.

10.4. Оценка выполнения Участниками и Операторами УПИ требований к обеспечению защиты информации

10.4.1. Участники и Операторы УПИ обеспечивают проведение оценки соответствия уровням защиты информации, установленным Положением Банка России №821-П (далее – «оценка соответствия защиты информации»).

10.4.2. Оценка соответствия защиты информации осуществляется в соответствии с положениями раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.2-2018 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 28 марта 2018 года N 156-ст "Об утверждении национального стандарта Российской Федерации" (М., ФГУП "Стандартинформ", 2018).

Оценка соответствия защиты информации должна осуществляться с привлечением организаций, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации для проведения работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного постановлением Правительства Российской Федерации от 3 февраля 2012 года №79 «О лицензировании деятельности по технической защите конфиденциальной информации» (далее – «проверяющая организация»).

В целях обеспечения защиты информации Участники, являющиеся операторами по переводу денежных средств, и Операторы УПИ должны хранить результат оценки соответствия защиты информации, подготовленный проверяющей организацией в виде отчета, не менее 5 (пяти) лет, начиная с даты его выдаче проверяющей организацией.

10.4.3. Участники, являющиеся операторами по переводу денежных средств, и Операторы УПИ обеспечивают проведение оценки соответствия защиты информации не реже одного раза в 2 (два) года.

10.4.4. Для целей анализа и контроля (мониторинга) обеспечения защиты информации в Системе Оператор устанавливает требования к содержанию, форме и периодичности представления информации, направляемой Субъектами Оператору. Требования по информированию Оператора установлены в «Порядке информирования Оператора Платежной системы МАРЛИН об обеспечении защиты информации» (Приложение №5) и обязательны для исполнения всеми Субъектами Платежной системы.

10.4.5. В случае подключения к Системе операционного центра, находящегося за пределами Российской Федерации, Оператор может определить иной состав информации, направляемой Оператору таким операционным центром.

10.5. Обеспечение совершенствования защиты информации

10.5.1. Субъекты обеспечивают пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, в связи:

- с изменениями требований к защите информации, определенных настоящими Правилами;
- изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России.

10.5.2. В случае наступления событий, влияющих на необходимость пересмотра и совершенствования порядка обеспечения защиты информации, Оператор направляет Субъектам соответствующее уведомление с указанием причин. Субъекты обязаны в течение 30 дней предоставить Оператору отчет о результатах пересмотра порядка обеспечения защиты информации в рамках своих обязанностей.

10.5.3. Субъекты регламентируют порядок принятия мер, направленных на совершенствование защиты информации, в случаях:

- изменения требований к защите информации, определенных настоящими Правилами;
- изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе;
- изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств;
- выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- выявления недостатков при проведении оценки соответствия.

10.6. Мероприятия по противодействию осуществлению Переводов без добровольного согласия клиента

10.6.1. Оператор Системы при реализации мероприятий по противодействию осуществлению Переводов без добровольного согласия клиента выполняет следующие действия:

- создает систему выявления и мониторинга переводов денежных средств по противодействию переводов денежных средств без добровольного согласия клиента в Платежной системе на основе признаков осуществления перевода денежных средств без добровольного согласия клиента, размещенных на официальном сайте Банка России в сети "Интернет" в соответствии с частью 3^3 статьи 8 Федерального закона № 161-ФЗ;
- определяет порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия Клиента для Участников;

- определяет признаки осуществления переводов денежных средств без добровольного согласия клиента на основании анализа выявленных операций по переводу денежных средств без добровольного согласия клиента и оценки риска совершения таких операций в рамках Платежной системы;
- использует выявленную Оператором Системы информацию о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Участников и (или) его Клиентов, применительно к своей инфраструктуре в целях противодействия осуществлению переводов денежных средств без добровольного согласия Клиента.

10.6.2. Система выявления и мониторинга переводов денежных средств без добровольного согласия клиента Оператора основывается на признаках осуществления операций без добровольного согласия клиента. Для получения указанной информации Оператор использует техническую инфраструктуру (автоматизированную систему) Банка России, информация о которой размещается на официальном сайте Банка России в сети "Интернет". Информация, предоставляемая Банком России, в т.ч. устанавливаемые Банком России признаки осуществления перевода без добровольного согласия клиента, интегрируется и(или) загружается в ПО Системы. Оператор на основе анализа операций, совершаемых в Системе, самостоятельно определяет признаки осуществления переводов денежных средств без добровольного согласия клиента и оценивает риски совершения таких операций в рамках Платежной системы.

10.6.3. Процедуры выявления и мониторинга переводов денежных средств без добровольного согласия клиента совмещены с процедурами приема к исполнению распоряжений.

10.6.4. Оператор по переводу денежных средств, являющийся Участником, при реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия Клиента должен применять полученную от Банка России информацию, содержащуюся в базе данных о случаях и попытках осуществления переводов денежных средств без добровольного согласия клиента, в целях выявления операций, соответствующих признакам осуществления переводов денежных средств без добровольного согласия клиента, выполнять мероприятия, предусмотренные Указанием Банка России №6828-У, а также:

- выявлять операции по переводу денежных средств, совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры Оператора по переводу денежных средств;
- осуществлять сбор сведений обо всех обращениях Клиентов (Отправителя, Получателя) о случаях и(или) попытках осуществления переводов денежных средств без добровольного согласия Клиента, в том числе при обращении Клиентов в федеральные органы исполнительной власти в сфере внутренних дел (при получении от Клиента таких сведений);
- обеспечить прием обращений Клиентов (Отправителя, Получателя) о случаях и (или) попытках осуществления переводов денежных средств без добровольного согласия Клиента и их регистрацию;
- 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 добровольного согласия Клиента, и фиксировать их;
- рассматривать случаи и (или) попытки осуществления переводов денежных средств без добровольного согласия Клиента, вызванные компьютерными атаками, направленные на объекты информационной инфраструктуры участников информационного обмена;
- осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их Клиентов, при их наличии;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак,

направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их Клиентов;

- реализовывать в отношении Клиента - получателя средств, в адрес которого ранее совершались операции по переводу денежных средств без добровольного согласия Клиента, в случаях, предусмотренных договором с Клиентом, содержащим условия указанного в части 1 статьи 9 Федерального закона №161-ФЗ договора об использовании электронного средства платежа, ограничения по параметрам (на сумму одной операции, общую сумму выдачи, период времени) операций по осуществлению переводов денежных средств с использованием Электронных средств платежа (переводов Электронных денежных средств), а также ограничения на получение и внесение наличных денежных средств в банкоматах и (или) кассах (пунктах обслуживания) оператора по переводу денежных средств;

- приостанавливать использование Клиентом (Отправителем, Получателем) электронного средства платежа в соответствии с частями 11.6 и 11.7 статьи 9 Федерального закона №161-ФЗ;

- реализовывать процедуру применения технического протокола, полученного в соответствии с пунктом 4.9 Указания Банка России №6828-У, а также реализовывать в отношении Клиента (Отправителя, Получателя) ограничения по параметрам (на сумму одной операции, общую сумму выдачи, период времени) операций по осуществлению переводов Электронных денежных средств с использованием Электронных средств платежа, ограничения на получение наличных денежных средств в банкоматах и (или) кассах (пунктах обслуживания) Оператора по переводу денежных средств;

- при выявлении информации о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Участника и (или) его Клиентов, осуществлять мероприятия по противодействию осуществлению переводов денежных средств без добровольного согласия Клиента в соответствии с пунктом 6.1 раздела 6 национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер", утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 8 августа 2017 года N 822-ст "Об утверждении национального стандарта" и введенного в действие 1 января 2018 г.

10.6.5. Оператор УПИ при реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента должен:

- реализовывать меры по противодействию осуществлению переводов денежных средств без добровольного согласия клиента (Участника) в соответствии с порядком, установленным Оператором;

- 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 добровольного согласия клиента;

- рассматривать случаи и (или) попытки осуществления переводов денежных средств без добровольного согласия клиента, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры участников информационного обмена;

- осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры операторов по переводу денежных средств, Операторов УПИ, операторов платежных систем и (или) их клиентов, при их наличии;

- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов;

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

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

10.6.7. Порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия Клиента для Участников:

- при выявлении операций, имеющих признаки осуществления перевода денежных средств без добровольного согласия Клиента, программным способом (посредством ПО Системы) выдается предупреждение о наличии таких признаков и блокируется возможность совершения такой операции до момента получения от Участника информации о дальнейших действиях. Переводу присваивается соответствующий статус;
- Участник при получении предупреждения обязан приостановить прием к исполнению распоряжения Клиента (за исключением операции с использованием платежных карт, перевода Электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России) на 2 (два) дня, либо отказать в совершении операции (в случае если операция совершается с использованием платежных карт, перевода Электронных денежных средств или перевода денежных средств с использованием сервиса быстрых платежей платежной системы Банка России);
- после приостановления/отказа в совершении операции Участник обязан незамедлительно предоставить Клиенту информацию, предусмотренную Федеральным законом №161-ФЗ, а также выполнить иные действия, предусмотренные Федеральным законом №161-ФЗ с соблюдением установленных в нем сроков.
- Участник незамедлительно информирует Оператора о факте приостановления операции Клиента или об отказе в ее совершении (в зависимости от способа осуществления операции), путем направления информационного сообщения по Согласованным каналам связи;
- после получения информации от Участника о возможности возобновления приема распоряжения Клиента к исполнению и(или) о намерении Клиента совершить повторную операцию Оператор незамедлительно возобновляет исполнение распоряжения, за исключением случаев, предусмотренных Федеральным законом №161-ФЗ;
- в случае, если Участник не направляет Оператору Системы подтверждение операции по истечении сроков, предусмотренных Федеральным законом №161-ФЗ, приостановленное ранее распоряжение Клиента считается не принятым, а повторная операция не совершенной;
- в случае, если Участник ошибочно направил подтверждение операции при получении отказа Клиента на совершение операции, Участник в день ошибочного подтверждения операции обязан сообщить Оператору по Согласованным каналам связи информацию о необходимости аннулирования приостановленного распоряжения. При наличии возможности (если Перевод не выдан, не зачислен Получателю, отсутствуют иные причины, препятствующие отмене ошибочно подтвержденной операции) Оператор не позднее текущего операционного дня, в котором совершено ошибочное подтверждение операции, возвращает Перевод в соответствующий статус.

10.6.8. Участники, Оператор Системы и Операторы УПИ информируют Банк России о Переводах без добровольного согласия клиентов в случаях и в порядке, предусмотренных Указанием Банка России №6828-У.

11. ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

11.1. Термины и определения

11.1.1. Настоящий порядок электронного документооборота (далее – «Порядок»), устанавливает правила осуществления обмена электронными сообщениями в Платежной системе МАРЛИН. Сторонами электронного документооборота в Платежной системе МАРЛИН являются:

- Оператор и Участники;
- Оператор и лица, привлеченные Участниками для осуществления операций с использованием Платежной системы МАРЛИН на основании отдельных договоров с ними;
- Оператор и платежные системы, с которыми у Оператора заключены договоры о межсистемном взаимодействии (если иное не указано в договорах с платежными системами).

Стороны электронного документооборота, предусмотренные настоящим Порядком, именуются по отдельности как «Сторона» или «участник[1]», а при совместном упоминании – «Стороны» или «участники».

11.1.2. Термины, применяемые в тексте настоящего раздела, используются в следующем значении:

Аккредитация Удостоверяющего центра - признание соответствия Удостоверяющего центра требованиям, предусмотренным Федеральным законом №63-ФЗ от 06.04.2011 «Об электронной подписи».

Владелец Сертификата Ключа проверки ЭП (далее – «Владелец Сертификата») – Сторона или сотрудник одной из Сторон, которому в установленном порядке Федеральным законом №63-ФЗ от 06.04.2011 «Об электронной подписи» выдан сертификат ключа проверки электронной подписи (в т.ч. сертификат ключа проверки электронной подписи от аккредитованного Удостоверяющего центра).

Информационная система – информационные ресурсы Оператора Платежной системы, в которых Стороны осуществляют Электронный документооборот, а также информационные ресурсы участников, используемые для обмена электронными сообщениями с Оператором.

Усиленная квалифицированная Электронная подпись (далее – «УКЭП») - электронная подпись (информация в электронной форме), которая присоединена к Электронному сообщению (подписываемой информации) и которая получена в результате криптографического преобразования информации с использованием Ключа электронной подписи, позволяет определить лицо или Сторону, подписавшее Электронный документ, позволяет обнаружить факт внесения изменений в Электронный документ после момента его подписания, Ключ проверки Электронной подписи указан в квалифицированном Сертификате, для создания и проверки электронной подписи используются Средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в соответствии с Федеральным законом №63-ФЗ от 06.04.2011 «Об электронной подписи».

Ключ ЭП – уникальная последовательность символов, предназначенная для создания ЭП.

Ключ проверки ЭП – уникальная последовательность символов, однозначно связанная с Ключом ЭП и предназначенная для проверки подлинности ЭП.

Компрометация Ключа ЭП – утрата доверия к тому, что используемый Ключ ЭП обеспечивает безопасность информации; выявление владельцем Ключа ЭП обстоятельств, при которых возможно несанкционированное использование данного ключа неуполномоченными лицами.

Корректная ЭП – ЭП, сформированная одной Стороной с использованием Ключа ЭП данной Стороны, соответствующая положительному результату ее проверки Ключом проверки ЭП той же Стороны.

[1] В дальнейшем в настоящем разделе под участниками понимаются в том числе привлеченные Участниками Партнеры и БПА (БПСА).

Усиленная неквалифицированная электронная подпись (далее – «УНЭП») – электронная подпись (информация в электронной форме), которая присоединена к Электронному сообщению (подписываемой информации) и которая получена в результате криптографического преобразования информации с использованием Ключа электронной подписи, позволяет определить лицо или Сторону, подписавшее Электронный документ, позволяет обнаружить факт внесения изменений в Электронный документ после момента его подписания, создается с использованием Средств электронной подписи.

Отправляющая сторона - Сторона электронного взаимодействия, которая направляет ЭД с использованием Информационной системы.

Пользователь – работник (сотрудник) участника, использующий Информационную систему Оператора в соответствии с документацией на нее.

Принимающая сторона - Сторона электронного взаимодействия, которой ЭД отправлен с использованием Информационной системы.

Сертификат Ключа проверки электронной подписи (Сертификат) - электронный документ или документ на бумажном носителе, сформированный участником и/или выданный Удостоверяющим центром, и подтверждающий принадлежность Ключа проверки Электронной подписи Владельцу Сертификата Ключа проверки Электронной подписи.

Средства электронной подписи (СЭП) – аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций - создание Электронной подписи в Электронном документе, проверка Электронной подписи в Электронном документе, создание Ключа Электронной подписи и Ключа проверки Электронной подписи.

Точка информационного обмена – точка доступа между Информационной системой участника и/или рабочим местом Пользователя и Информационными системами Оператора.

Удостоверяющий центр – юридическое лицо, индивидуальный предприниматель либо государственный орган или орган местного самоуправления, осуществляющие функции по созданию и выдаче сертификатов ключей проверки электронных подписей, а также иные функции, предусмотренные Федеральным законом №63-ФЗ от 06.04.2011 г. «Об электронной подписи».

Усиленная Электронная подпись (УЭП) – Усиленная неквалифицированная электронная подпись (УНЭП) или Усиленная квалифицированная Электронная подпись (УКЭП).

Электронная подпись (далее – ЭП) – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию.

В ПС используются УНЭП и УКЭП.

Электронный документ (ЭД) – электронное сообщение, подписанное ЭП Оператора, Участника или привлеченного им лица и имеющее равную юридическую силу с расчетными и иными документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати.

Электронное сообщение (ЭС) – логически целостная совокупность структурированных данных, имеющих смысл для участников информационного взаимодействия. Информация в Электронном сообщении представлена в электронно-цифровой форме, позволяющей обеспечить ее обработку средствами вычислительной техники, передачу по каналам связи и хранение на машиночитаемых носителях информации.

11.1.3. Иные термины и определения, содержащиеся в тексте настоящего Порядка, трактуются в соответствии с терминами и определениями, содержащимися в Правилах.

11.2. Общие положения

11.2.1. В Порядке устанавливаются общие принципы осуществления информационного взаимодействия с использованием электронного документооборота между Сторонами, требования к оформлению и содержанию Электронных документов, их форматам и реквизитам, особенности порядка их обработки, исполнения и хранения.

11.2.2. Применяемые в Системе средства защиты обеспечивают осуществление Сторонами обмена ЭД с использованием общедоступных каналов связи и нескомпрометированных ключей.

11.2.3. Использование соответствующей Информационной системы Оператора для обмена ЭД в целях работы в Системе осуществляется участниками согласно пп. 11.8.6 – 11.8.9 Порядка на основании заявления о предоставлении доступа и доводится до сведения участника по Согласованным каналам связи. Заявление о предоставлении доступа предусматривает разграничение ролей прав доступа для совершения действий в Информационной системе Оператора и определяет объем полномочий, необходимых для той или иной роли. Участник предоставляет Оператору Сертификат и подтверждает, что Владелец Сертификата является лицом, надлежащим образом уполномоченным на совершение операций в Информационной системе Оператора от имени участника, предусмотренных для выполнения пользователем с соответствующей ролью.

11.2.4. ЭД, подписанные Владельцами Сертификатов Ключа проверки УЭП, юридически эквивалентны соответствующим документам, выполненным на бумажном носителе, подписанным руководителем (иным уполномоченным представителем) и имеющем оттиск печати данной Стороны, обладают полной юридической силой и являются основанием возникновения соответствующих прав и обязанностей Сторон, вытекающих из данного ЭД, если соблюдены следующие условия:

- Сертификат УНЭП изготовлен одной Стороной/Удостоверяющим центром и подтвержден другой Стороной, и/или Сертификат УКЭП изготовлен аккредитованным Удостоверяющим центром, и не утратили силу (действуют) на момент проверки подлинности подписи ЭД или на момент подписания ЭД;
- подтверждена подлинность этих ЭП;
- Владелец Сертификата Ключа проверки ЭП уполномочен от имени Отправляющей стороны подписывать расчетные и иные документы на бумажных носителях.

11.2.5. Единой шкалой времени при осуществлении ЭДО является московское поясное время. Контрольным является время системных часов аппаратных средств Операционного центра.

11.2.6. ЭДО между Сторонами, направленный на обмен ЭД, осуществляется и используется в рамках Информационных систем Оператора, а также между информационными системами Оператора и участника, к которым интегрируется Оператор, или в которые интегрируется участник.

11.2.7. Обмен информацией, не носящей платежный характер и не содержащей банковскую тайну, осуществляется Сторонами по Согласованным каналам связи, указанным Стороной в соответствующем заявлении, через операторов электронного документооборота, или с использованием Информационной системы Оператора (при наличии технической возможности).

11.2.8. Обмен ЭД между Оператором и привлеченными Операторами УПИ осуществляется в соответствии с заключенными между ними договором.

11.3. Электронные сообщения и документы

11.3.1. Категории Электронных сообщения:

11.3.1.1. Электронные сообщения подразделяются на следующие категории:

- Категория 1 - Электронные сообщения, требующие наличие ЭП Отправляющей стороны и не требующие ответа.
- Категория 2 - Электронные сообщения, требующие наличие ЭП Отправляющей стороны и требующие ответа, не содержащего ЭП Принимающей стороны.

- Категория 3 - Электронные сообщения, требующие наличие ЭП Отправляющей стороны и требующие ответа, подписанного ЭП Принимающей стороны.

11.3.1.2. Все отправляемые Сторонами сообщения являются Электронными документами, т.е. относятся к категориям 1-3.

11.3.2. Условия признания Электронного сообщения отправленным:

ЭС считается отправленным Отправляющей стороной в случае успешного завершения технических функций отправки. Техническая функция отправки считается завершенной, если ЭС и/или ЭД покинул(о) информационную систему Отправляющей стороны и было успешно передано в информационную систему ЭДО Принимающей стороны. Датой и временем отправки считаются дата и время завершения технических функций отправки.

11.3.3. Условия признания Электронного сообщения полученным:

Электронное сообщение считается полученным Принимающей стороной в случае:

- Для Категории 1 – в момент его успешной отправки Отправляющей стороной.
- Для Категории 2 – в момент его получения Принимающей стороной. Датой и временем приема считаются дата и время его получения.
- Для Категории 3 - в момент получения Отправляющей стороной ответа от Принимающей стороны. Датой и временем приема считаются дата и время получения сообщения Принимающей стороной.

11.3.4. Условия принятия Электронных сообщений в обработку Принимающей стороной:

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

- Для сообщений, обмен которых происходит с использованием шифрования, сообщение успешно расшифровано;
- Сообщение относится к Категории 1, 2 или 3, имеет ЭП и положительный результат ее проверки.
- Электронное сообщение надлежащим образом оформлено, т.е. его формат соответствует формату такого сообщения, предусмотренному на момент формирования документа технологией Системы.

11.4. Условия организации и правила осуществления ЭДО

11.4.1. Формирование ЭС осуществляется в следующем порядке:

- формирование ЭС в формате, установленном для данного ЭС;
- подписание сформированного ЭС соответствующим видом ЭП (при необходимости);
- шифрование ЭС (при необходимости);
- отправка ЭС.

11.4.2. Проверка подлинности ЭП осуществляется путем проверки Сертификата Ключа проверки ЭП с использованием специального программного обеспечения (например, КриптоПро, КриптоАрм) или интернет-сервисов (https://e-trust.gosuslugi.ru/check/sign#/portal/sig-check), или путем обращения в Удостоверяющий центр в целях подтверждения корректности примененной ЭП.

11.4.3. Проверка подлинности доставленного ЭС включает:

- расшифровку ЭС (при необходимости);
- проверку ЭС на соответствие установленному для него формату;
- проверку подлинности ЭП ЭС (при её наличии).

В случае положительного результата проверки ЭС, данное ЭС признается надлежащим. В противном случае ЭС считается не полученным, о чем Принимающая сторона может направить уведомление Отправляющей стороне.

11.4.4. Порядок создания ЭП регламентируется правилами Оператора по выработке, обмену, смене Ключей ЭП и действиями при компрометации Ключа ЭП, которые Стороны безусловно признают и считают достаточными для подтверждения выполненных действий в Системе. Создание Корректной ЭП для ЭД, исходящего от одной из Сторон, невозможно без знания Ключа ЭП данной Стороны.

11.4.5. Сторона обязуется предоставить другой Стороне Сертификат Ключа проверки ЭП, который будет использоваться при информационном обмене. Стороны обязуются хранить Сертификат Ключа проверки ЭП в соответствии с внутренними правилами хранения ключевых носителей каждой из Сторон и/или Удостоверяющего центра в течение всего срока хранения Электронных документов, подписанных соответствующими Ключами ЭП.

11.4.6. Сертификат, сформированный Пользователем и/или Стороной (в случае УНЭП) или квалифицированный Сертификат ключа проверки ЭП, выданный аккредитованным Удостоверяющим центром (в случае УКЭП), и переданный согласно правилам Оператора по выработке, обмену, смене ключа ЭП и действиям при компрометации ключа ЭП другой Стороне, принадлежит этой же Стороне, если Сторона письменно не заявила о его недействительности.

11.4.7. Стороны используют Сертификат с даты регистрации ЭП в Системе до даты прекращения действия ЭП.

11.4.8. Плановая/внеплановая смена Ключей ЭП производится в соответствии с регламентом аккредитованного Удостоверяющего центра (для УКЭП) и (или) правилам Оператора по выработке, обмену, смене ключа ЭП и действия при компрометации ключа ЭП (для УНЭП).

11.4.9. После ввода в действие новых Ключей ЭП, Стороны обязуются обеспечивать конфиденциальность при хранении аннулированных Ключей ЭП в течение всего срока хранения документов, подписанных соответствующими Ключами ЭП.

11.4.10. Стороны гарантируют, что:

- не используют Сертификат, если им известно, что Ключ ЭП стал скомпрометированным;
- каждая Сторона несет ответственность за действия своих работников, в том числе за действия уполномоченного лица при направлении ЭД;
- обеспечат хранение и конфиденциальность собственных Ключей ЭП в тайне и примут все необходимые меры для предотвращения Компрометации Ключа ЭП в процессе хранения и использования.

11.4.11. ЭД, исходящие от одной из Сторон, без ЭП данной Стороны, или подписанные ЭП, о компрометации ключа которой было сообщено отправившей Стороной до момента получения ЭД, не имеют юридической силы, Сторонами не рассматриваются и не исполняются.

11.4.12. Если результат проверки ЭД, подписанного ЭП, дает отрицательный результат, то указанный ЭД становится некорректным.

11.4.13. ЭД, формируемые Сторонами в соответствии с заключенными договорами в целях осуществления операций с использованием Платежной системы МАРЛИН (далее – «Договор»), заверенные ЭП одной из Сторон, юридически эквивалентны соответствующим документам, выполненным на бумажном носителе, подписанным руководителем (иным уполномоченным представителем) и имеющим оттиск печати данной Стороны, обладают полной юридической силой и являются основанием возникновения соответствующих прав и обязанностей Сторон, вытекающих из данного ЭД, при условии, что к моменту получения ЭД другой Стороной Сторона, отправившая ЭД, не сообщила о компрометации своей ЭП.

11.4.14. Стороны признают, что одной ЭП могут быть подписаны несколько связанных между собой ЭД (пакет электронных документов). При подписании ЭП пакета ЭД каждый из ЭД, входящих в этот пакет, считается подписанным ЭП того вида, которой подписан пакет ЭД.

11.4.15. ЭД с ЭП одной из Сторон принимаются Сторонами в качестве доказательств для решения спорных вопросов в порядке, указанном в разделе 11.6 Порядка. ЭД, не имеющие Корректной ЭП, в качестве доказательств при решении спорных вопросов Сторонами не используются и не рассматриваются.

11.4.16. Учет Электронных документов:

- Учет ЭД осуществляется путем ведения электронных баз учета ЭД. Технология ведения электронных баз учета ЭД должна включать программно-технологические процедуры заполнения и администрирования электронных журналов и средства хранения этой информации. Программные средства ведения электронных баз учета ЭД являются составной частью программного обеспечения, используемого для организации ЭДО.
- Выполнение работ по ведению учета ЭД возлагается на подразделение, определяемое каждой Стороной самостоятельно[1].
- Оператор и участники обеспечивают защиту от несанкционированного доступа и непреднамеренного уничтожения и/или искажения учетных данных, содержащихся в электронных базах учета ЭД. Срок хранения учетных данных не может быть менее 5 лет.

11.4.17. Хранение электронных документов:

- Все учтенные ЭД должны храниться в течение сроков, предусмотренных Правилами Системы. ЭД должны храниться либо в электронных архивах, либо в виде копий ЭД на бумажных носителях, заверенных ответственным лицом Стороны.
- Если Правилами Системы не предусмотрено иное, ЭД должны храниться в том же формате, в котором они были сформированы, отправлены или получены. Срок хранения ЭД не может быть менее 5 лет.
- Хранение ЭД должно сопровождаться хранением соответствующих электронных журналов учета, Сертификатов ключей проверки ЭП и программного обеспечения, обеспечивающего возможность работы с электронными журналами и проверки ЭП, хранимых ЭД.
- Обязанности хранения ЭД возлагаются на Стороны.
- Для выполнения текущих работ по ведению электронных архивов в системах обработки данных Стороны назначают ответственных лиц.
- Электронные архивы подлежат защите от несанкционированного доступа и непреднамеренного или преднамеренного уничтожения и/или искажения.

11.4.18. Копии Электронного документа на бумажном носителе:

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

11.5. Обеспечение информационной безопасности при ЭДО

11.5.1. Общие положения информационной безопасности:

[1] Выполнение работ по ведению учета ЭД Оператора возлагается на подразделение информационных технологий

11.5.1.1. Оператор обеспечивает информационную безопасность при информационном взаимодействии участников в соответствии с Правилами Системы.

11.5.1.2. Участники самостоятельно обеспечивают информационную безопасность при организации ЭДО внутри своей корпоративной Информационной системы.

11.5.2. Для криптографической защиты информации в Системе применяются:

11.5.2.1. СКЗИ, реализующие иностранные криптографические алгоритмы и криптографические алгоритмы, определенные национальными стандартами Российской Федерации, имеющие подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;

11.5.2.2. Криптографический протокол SSL/TLS используется в форме протокола https (прикладной протокол http поверх криптографического протокола SSL/TLS).

11.5.3. Общие условия работы с ключевой информацией:

11.5.3.1. Стороны при действиях по выработке, смене и компрометации Ключа ЭП руководствуются правилами Оператора и/или Удостоверяющего центра.

11.5.3.2. Правила Оператора включены в техническую документацию Оператора ПС по подключению к ПС и доводится до сведения Участника в ЛК или по Согласованным каналам связи.

11.5.3.3. Выполнение требований Оператора и/или Удостоверяющего центра при работе с ключевой информацией обязательно для всех участников.

11.5.3.4. Участники самостоятельно вырабатывают криптографические Ключи ЭП и обеспечивают работу с ключевой информацией.

11.5.3.5. Владелец Сертификата Ключа проверки ЭП должен быть уполномочен подписывать расчетные и иные документы на бумажных носителях от имени Отправляющей стороны на момент отправки подписанного ЭД. Передавая Оператору Сертификат Ключа проверки ЭП, участник подтверждает, что его Владелец наделен необходимыми и достаточными полномочиями для совершения операций в Системе от имени участника.

11.5.3.6. При проверке документов для регистрации Сертификата Ключа проверки ЭП за участником и/или Пользователем, Оператор Системы в полном объеме проверяет данные участника и/или Пользователя, полномочия уполномоченного лица на право осуществления действий от имени участника в рамках Системы.

11.5.3.7. Владелец Сертификата Ключа проверки ЭП несёт ответственность за достоверность сведений, которые были предоставлены им Оператору Системы при создании и регистрации Сертификата Ключа проверки Электронной подписи.

11.5.3.8. Владелец Сертификата Ключа проверки ЭП хранит собственные Ключи Электронной подписи в тайне и принимает все необходимые меры для предотвращения их компрометации в процессе хранения и использования.

11.5.3.9. Стороны обязаны хранить в тайне и не передавать третьим лицам информацию о своих Ключах ЭП, используемых в Системе, не использовать при обмене ЭД Ключи ЭП, использовавшиеся ими ранее или использующиеся в текущее время иными лицами, а также Ключи ЭП, в отношении которых у Сторон имеются обоснованные подозрения, достоверные подтверждения или полученные сообщения о Компрометации.

11.5.3.10. Владельцы Сертификата Ключа проверки ЭП хранят выданные им Сертификаты Ключей, в том числе и по истечении срока действия сертификата.

11.5.3.11. В каждой Точке информационного обмена может использоваться один и только один действующий Ключ ЭП.

11.5.4. Действия в случае Компрометации ключей:

11.5.4.1. В случае Компрометации ключей ЭП Владелец Сертификата Ключа проверки ЭП обязан незамедлительно уведомить Оператора Системы о компрометации его ключа, указав скомпрометированный ключ. Датой и временем Компрометации считаются дата и время получения Оператором Системы уведомления о Компрометации согласно правилам Оператора по выработке, обмену, смене ключа ЭП и действиям при компрометации ключа ЭП.

11.5.4.2. Все действия в Системе с использованием скомпрометированных ключей ЭП немедленно прекращаются.

11.5.4.3. Электронный документ, подписанный скомпрометированным ключом ЭП, признается ненадлежащим.

11.5.4.4. Участник после уведомления Оператора Системы о компрометации ключа осуществляет процедуры в соответствии с правилами Оператора и/или Удостоверяющего центра: вырабатывает новый Ключ и отправляет запрос на его сертификацию.

11.5.4.5. Стороны обязуются оформить и передать другой Стороне новый Сертификат Ключа проверки УНЭП не позднее дня, следующего за днем уведомления о компрометации ключа УНЭП, и новый Сертификат Ключа проверки УКЭП не позднее 3 (трех) рабочих дней, следующего за днем уведомления о компрометации ключа УКЭП.

11.6. Порядок разрешения конфликтных ситуаций, связанных с использованием ЭДО в Платежной системе МАРЛИН

11.6.1. Споры и разногласия, связанные с использованием ЭДО, расчетами в электронной форме и применением средств шифрования и ЭП, решаются путем переговоров.

11.6.2. В случае возникновения конфликтной ситуации по поводу авторства и(или) подлинности текста ЭД, которую не удается решить путем переговоров, Оператором Системы организуется проведение технической экспертизы спорного ЭД.

11.6.3. Разбор конфликтной ситуации выполняется по инициативе любой Стороны и включает:

- предъявление претензии;
- образование экспертной комиссии;
- разбор конфликтной ситуации;
- выработка заключения и решения по конфликтной ситуации.

11.6.4. Разбор конфликтной ситуации заключается в доказательстве принадлежности или не принадлежности ЭП конкретного ЭД со всеми его реквизитами конкретному Владельцу Сертификата ключа проверки ЭП.

11.6.5. Проведение технической экспертизы организуется Оператором на основании письменного заявления заинтересованной Стороны.

11.6.6. Заявление о споре подается Оператору в письменной форме с указанием наименования заявителя, наименования и реквизитов спорного ЭД, требований заявителя, обстоятельств, на которых заявитель основывает свои требования, перечня прилагаемых к заявлению документов. К заявлению также прилагается список должностных лиц заявителя, предлагаемых для включения в состав экспертной комиссии.

11.6.7. Для проведения технической экспертизы Оператор создает комиссию, включающую равное количество, но не менее двух, представителей от Оператора и от каждой из заинтересованных сторон. В состав комиссии по соглашению сторон включаются представители служб информационной безопасности заинтересованных сторон. В состав комиссии могут включаться независимые технические эксперты. В состав комиссии может включаться представитель аккредитованного Удостоверяющего центра, в случае использования УКЭП (при необходимости).

11.6.8. В течение 5 (пяти) рабочих дней Оператор обязан уведомить все имеющие отношение к рассматриваемому документу или вопросу Стороны о месте и времени проведения экспертизы и составе экспертной комиссии.

11.6.9. Каждая из Сторон вправе заявить об отводе эксперта из состава экспертной комиссии, если есть основания предполагать, что он прямо или косвенно заинтересован в исходе дела.

11.6.10. Оператор и экспертная комиссия принимают меры к тому, чтобы экспертиза была проведена в срок не более 5 (пяти) рабочих дней со дня поступления заявления. В исключительных случаях срок может быть продлен, но не более чем на 7 (семь) рабочих дней.

11.6.11. Неявка любой из спорящих Сторон, надлежащим образом извещенных о месте и времени проведения экспертизы, не препятствует проведению экспертизы, если отсутствующая Сторона не представила письменную просьбу отложить проведение экспертизы по уважительной причине, но на срок не более 2 (двух) рабочих дней.

11.6.12. Экспертная комиссия проводит экспертизу только после получения всех необходимых материалов, как правило, на территории и в помещении Оператора.

11.6.13. Для проведения технической экспертизы в комиссию передаются (в зависимости от типа проверяемой ЭП):

- электронный документ, подписанный ЭП, подлинность которой оспаривается;
- запрос на выведение из действия ключа, если таковой был;
- Сертификаты Ключей проверки ЭП Владельцев Сертификатов, подписавших документ;
- справочник сертификатов с Сертификатом Владельца, подпись которого оспаривается (для УКЭП);
- съемные носители с файлами контрольных сумм исполняемых модулей СКЗИ Сторон, участвующих в споре;
- электронные журналы (архивы журналов).

11.6.14. Экспертная комиссия устанавливает на персональный компьютер эталонную операционную систему и эталонное программное обеспечение, хранящееся у Оператора. Компьютер не должен иметь установленного на нем программного обеспечения. С этой целью его жесткий диск может форматироваться в присутствии всех членов экспертной комиссии.

11.6.15. Экспертная комиссия проверяет целостность программного обеспечения спорящих Сторон путем сравнения с эталонным программным обеспечением, хранящимся у Оператора.

11.6.16. Для разбора конфликта по поводу авторства и(или) подлинности текста документа, подписанного ЭП, экспертная комиссия осуществляет следующие действия:

- проверяет актуальность Сертификата Ключа проверки ЭП;
- сравнивает содержание однотипных экземпляров Сертификатов, представленных Оператором или Участником и Удостоверяющим центром, в случае использования УЭП;
- проверяется подлинность ЭП спорного документа.

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

11.6.17. Протокол проверки подписи является основным документом работы экспертной комиссии и должен быть подписан всеми ее членами.

11.6.18. При рассмотрении конфликтной ситуации по поводу актуальности Сертификата Ключа проверки ЭП, когда одна Сторона утверждает, что на момент времени Т0 Сертификат Ключа проверки ЭП другой стороны был зарегистрирован, как действующий, а вторая Сторона считает, что Сертификат Ключа проверки ЭП на этот же момент Т0 был в установленном порядке выведен из действия, вторая Сторона должна представить экспертной комиссии уведомляющее сообщение о

выведении из действия спорного Ключа. При этом моменты наступления всех событий, имеющих отношение к возникшему по вопросу актуальности открытого ключа спору, указываются по времени Оператора.

Заключение экспертной комиссии, в котором указано, что время Т0 более позднее, чем время, указанное в названном уведомляющем сообщении, является доказательством факта недействительности спорного Ключа на момент времени Т0.

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

11.6.19. По итогам проведения экспертизы составляется письменное заключение, содержащее:

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

11.6.20. При проведении экспертизы при необходимости по ЭД могут быть изготовлены в установленном порядке их бумажные копии.

11.6.21. Экспертная комиссия не дает правовой оценки действиям Сторон.

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

11.6.23. В случае согласия с выводами экспертной комиссии Стороны, между которыми возник спор, заключают соглашение об урегулировании разногласий.

11.7. Используемые ЭС и ЭП в Информационных системах Оператора

11.7.1. ЭС, отправляемые участниками при использовании Информационной системы Оператора, используемой участниками для обслуживания Клиентов, в т.ч. каналы ДБО, относятся к Категориям 1 и 3;

11.7.2. ЭС, отправляемые участниками при использовании Информационной системы Оператора, содержащей информацию о доступных лимитах участника, тарифах, об осуществленных участником переводах, предоставляющей возможность участникам администрировать пункты обслуживания Клиентов, а также осуществлять иные действия, предусмотренные документацией Оператора, относятся к Категориям 1-3;

11.7.3. ЭС, отправляемые между Информационными системами Сторон, относятся к Категории 3;

11.7.4. ЭС, отправляемые Оператором при использовании Информационной системы Оператора для передачи Отчетов по итогам операционного дня (дней), относятся к Категории 1.

11.7.5. При обмене ЭД в рамках Информационных систем Оператора, указанных в п. 11.7.1 и 11.7.2 Порядка, используется УЭП, выданная на конкретного Пользователя или на участника.

11.7.6. При обмене ЭД в рамках Информационной системы Оператора, указанной в п. 11.7.3 и 11.7.4. Порядка используется УЭП, выданная на конкретное уполномоченное лицо или на участника.

11.8. Требования к техническому и программному обеспечению осуществления операций

11.8.1. Участники самостоятельно и за свой счет обеспечивают технические условия функционирования Информационных систем Оператора в своей корпоративной сети.

11.8.2. Информационные системы Оператора, с помощью которых осуществляется формирование ЭС и взаимодействие с Оператором, должны работать в соответствии с применяемой на момент совершения операций технологией Системы.

11.8.3. Технологии Системы включают в себя техническое и технологическое описание процедур и форматов взаимодействия Оператора с участниками.

11.8.4. Технологии Системы включены в техническую документацию Оператора, направляемую по Согласованным каналам связи или размещаемую в ЛК.

11.8.5. В случае изменения технологий Системы и необходимости замены или модификации Информационных систем Оператора участники извещаются путем направления по Согласованным каналам связи или размещения информации в ЛК.

11.8.6. Участник самостоятельно по согласованию с Оператором выбирает Информационные системы Оператора, которые он будет использовать. Оператор предоставляет доступы участнику на основании заявления о предоставлении доступа к техническим ресурсам Системы, форма которого размещается в ЛК или направляется по Согласованным каналам связи.

11.8.7. Оператор может рекомендовать участникам предоставляемые им для использования Информационные системы Оператора или ПО, поставляемое партнерами-разработчиками Системы.

11.8.8. Перед началом работы или смене Информационных систем Оператора участник в обязательном порядке проводит процедуры тестирования подключения.

11.8.9. Условия использования поставляемых Оператором Информационных систем Оператора:

- Инструкции по настройке доступов и использованию Информационных систем Оператора включены в техническую документацию Оператора или в инструкции пользователя и размещены в ЛК или направляются по Согласованным каналам связи;
- Технические характеристики содержатся в технической документации Оператора и размещены в ЛК или направляются по Согласованным каналам связи.
- Предоставляемые Оператором Информационные системы поставляются в виде «как есть»;
- Оператор самостоятельно определяет состав, порядок и сроки внесения изменений в свои Информационные системы;
- Прием официально заверенных заявок на доработки Информационных систем Оператора принимается Оператором по Согласованным каналам связи;
- Услуги по настройке и использованию поставляемых Информационных систем оказывает служба технической поддержки Оператора.

11.8.9.1. Условия использования прочего ПО:

- участники вправе самостоятельно или с привлечением сторонних организаций разработать и эксплуатировать ПО для взаимодействия с ПО Системы;
- Оператор может оказывать консультационные услуги в процессе разработки;
- разработанное таким образом ПО в обязательном порядке тестируется участником самостоятельно по методикам Оператора Системы;
- все риски, связанные с нарушением действующих на момент совершения операций технологий, несет участник.

- Оператор Системы не оказывает консультационной помощи сотрудникам участника по использованию разработанного таким образом ПО.

11.9. Права и обязанности Сторон при осуществлении ЭДО

11.9.1. Стороны обязаны:

11.9.1.1. Не позднее даты начала использования ПО Системы обменяться Сертификатами.

11.9.1.2. При получении ЭД, направленного другой Стороной, производить проверку Корректности ЭП Стороны, отправившей ЭД, проверку правильности заполнения реквизитов документа. Не принимать к исполнению ЭД с некорректной ЭП другой Стороны или с неполными/неверными реквизитами и не позднее следующего дня сообщать Стороне, от которой получен такой Электронный документ, о его неисполнении и о причинах неисполнения.

11.9.1.3. Исполнять ЭД с Корректной ЭП, полученные от другой Стороны по Системе, в соответствии с договором.

11.9.1.4. Незамедлительно (в течение одного часа) информировать любым доступным способом другую Сторону обо всех случаях возникновения технических неисправностей или других обстоятельств, препятствующих обмену ЭД. При устранении технических неисправностей Сторона обязуется сообщить другой стороне о возобновлении ЭДО.

11.9.1.5. При наличии оснований для предположения о Компрометации Ключа ЭП незамедлительно с момента получения информации:

- сообщить другой Стороне об обнаружении попытки несанкционированного доступа к Системе и/или Компрометации Ключа ЭП;
- требовать от другой Стороны приостановления действия Сертификата;
- направить другой Стороне уведомление об отмене действия Ключа ЭП и соответствующего ему Ключа проверки ЭП по форме Оператора.

11.9.1.6. Прекратить использование Сертификата, в отношении которого от другой Стороны получено уведомление об отмене действия Ключа ЭП и соответствующего ему Ключа проверки ЭП, представленного по форме, предусмотренной Оператором.

11.9.1.7. Регистрировать Сертификаты, присылаемые другой Стороной;

11.9.1.8. Обеспечить автоматизированную проверку действительности Ключа ЭП, не позволяющую подписать документ Ключом ЭП, действие которого прекращено.

11.9.1.9. Выполнять требования по оформлению и защите передаваемой информации в виде ЭД, защите Ключей ЭП и другой передаваемой и получаемой информации.

11.9.1.10. Обеспечивать доступ к средствам обмена ЭД только уполномоченным работникам Стороны.

11.9.2. Стороны вправе:

11.9.2.1. Досрочно прекратить действие своего Ключа ЭП и потребовать от другой Стороны блокировать указанный Сертификат, направив другой Стороне уведомление об отмене действия Ключа ЭП и соответствующего Ключа проверки ЭП по форме, предусмотренной Оператором.

11.9.2.2. В любое время по своему усмотрению генерировать новые Ключи ЭП и передать другой Стороне для регистрации нового Сертификата.

11.9.3. В случае технологической необходимости Оператор вправе вносить изменения в условия осуществления ЭДО в одностороннем порядке, предварительно уведомив Субъектов не менее чем за 14 (четырнадцать) календарных дней до момента вступления в силу изменений путем размещения информации в ЛК или направления информации по Согласованным каналам связи с последующим отражением указанных изменений в Правилах Платежной системы МАРЛИН.

11.10. Ответственность

11.10.1. Участник несет ответственность за соблюдение положений Порядка электронного документооборота, установленного Правилами, в соответствии с действующим законодательством Российской Федерации.

11.10.2. Участник обязуется обеспечить соблюдение правил ЭДО, установленных настоящим Порядком и иными документами Оператора, уполномоченным лицом и пользователями участника.

11.10.3. Участник несет ответственность за действия/бездействие уполномоченного лица и пользователей, как за свои собственные. Субъект не вправе в спорах ссылаться на ненадлежащее исполнение уполномоченным лицом и (или) пользователем своих обязательств.

11.10.4. В случае возникновения у Оператора убытков по вине уполномоченного лица/пользователя, участник обязуется компенсировать все причиненные убытки в полном объеме незамедлительно после получения письменного требования о возмещении убытков от Оператора.

11.10.5. Стороны, их уполномоченные лица и Пользователи не несут ответственности за неисправности линии связи или оборудования, приводящие к невозможности передачи ЭД.

11.10.6. Стороны не несут ответственности за неисполнение или ненадлежащее исполнение принятых по настоящему Порядку обязательств в случае возникновения обстоятельств непреодолимой силы, если Сторона, не выполнившая или выполнившая ненадлежащим образом свои обязательства в результате их влияния, доведет до сведения другой Стороны известие о случившемся в минимально возможный короткий срок после возникновения этих обстоятельств.

11.10.7. Оператор не несет ответственность за убытки Субъектов, возникшие в результате использования системы ЭДО неуполномоченными лицами Субъекта, если такое использование стало возможным по небрежности или умыслу Субъекта и/или соответствующего пользователя или третьих лиц.

11.10.8. Стороны признают используемые в системе ЭДО средства защиты информации достаточными для защиты от несанкционированного доступа и подтверждения подлинности ЭП в ЭД.

11.10.9. Стороны, их уполномоченные лица и Пользователи признают, что внесение произвольных изменений в ЭД влечет за собой отрицательный результат проверки подлинности ЭП в ЭД.

11.10.10. Стороны не несут ответственности за достоверность и правильность информации, указанной в ЭД, полученных от другой Стороны, при условии признания корректности ЭП другой Стороны, которая (корректность) признается достаточным требованием для подтверждения авторства и подлинности документов.

11.10.11. Сторона не несет ответственности за ущерб, понесенный другой Стороной в результате использования Ключа ЭП другой Стороны, о Компрометации которой другая Сторона не сообщила до момента отправки данной Стороне ЭД, подписанного этим Ключом ЭП.

11.10.12. Конфликтные ситуации, возникающие между Сторонами при использовании Системы, Стороны обязуются рассматривать и разрешать в соответствии с разделом 11.6 Правил. Стороны обязуются принимать результаты такого рассмотрения и нести ответственность в соответствии с условиями Договора и требованиями действующего законодательства согласно результатам рассмотрения конфликтной ситуации.

12. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ

12.1. Все Субъекты Системы обязаны принимать все доступные меры к разрешению споров и разногласий, возникающих в процессе взаимодействия в Платежной системе в рамках претензионной работы в досудебном порядке.

12.2. Досудебное урегулирование споров и разногласий, которые могут возникнуть между Оператором и Участниками, между Оператором и привлеченными Операторами УПИ, между Участниками и привлеченными Операторами УПИ в процессе исполнения сторонами своих обязанностей в рамках настоящих Правил, происходит путем проведения переговоров, в том числе путем обмена письмами, электронными сообщениями, проведением рабочих встреч и совещаний, а также путем совершения иных действий, направленных на урегулирование спора.

12.3. В случае возникновения спора между Оператором и Участником:

12.3.1. Сторона, имеющая возражения, незамедлительно извещает в письменном виде другую сторону об обстоятельствах, свидетельствующих о возникновении спорной ситуации, а также о предполагаемых причинах. Другая сторона обязана в течение 5 (пяти) рабочих дней проверить наличие указанных в извещении обстоятельств, и по необходимости принять меры по разрешению спорной ситуации, со своей стороны. В указанный выше срок сторона, которой направлена информация о спорной ситуации, извещает в письменном виде сторону, имеющую возражения о результатах проверки и, при необходимости, о мерах, принятых для разрешения спорной ситуации.

12.3.2. Спорная ситуация признается разрешенной в рабочем порядке в случае, если сторона, имеющая возражения, удовлетворена информацией, полученной в извещении от другой стороны, и не имеет к ней претензий в связи со спорной ситуацией.

12.3.3. В случае невозможности разрешения спора в рабочем порядке сторона направляет другой стороне письменную претензию, которая должна быть рассмотрена в срок, не превышающий 15 (пятнадцать) рабочих дней с даты ее получения ответчиком. В случае не достижения согласия в указанный в настоящем пункте срок инициатор обращается за разрешением спора в суд.

12.4. В случае возникновения спора между Оператором и привлеченным Оператором УПИ:

12.4.1. Стороны предпринимают усилия для разрешения спора в досудебном порядке, для чего применяются способы урегулирования спорной ситуации, предусмотренные п. 12.2 Правил, а также иные способы, если они предусмотрены договорами Оператора с привлеченными Операторами УПИ.

12.4.2. В случае недостижения сторонами спора соглашения о разрешении спора в досудебном порядке в течение 30 (тридцати) дней с даты направления стороной спора другой стороне спора заявления о споре, любая из сторон спора вправе обратиться в суд в соответствии положениями настоящих Правил.

12.5. В случае возникновения споров между привлеченными Операторами УПИ и Участниками:

12.5.1. Досудебное разрешение споров между привлеченным Операторами УПИ и Участниками происходит согласно условиям заключенных между ними договоров.

12.5.2. Для решения спорной ситуации стороны вправе привлечь Оператора, который может выступить арбитром в процедуре урегулировании спорной ситуации.

12.5.3. В случае привлечения к разрешению спора Оператора, последний запрашивает у участников спора первичные документы по спорной операции и (или) запрашивает соответствующую информацию у привлеченных Операторов УПИ. Данные в электронной форме, полученные от привлеченных Операторов УПИ, приравниваются в Системе к первичным расчетным документам.

12.5.4. При необходимости Оператор создает экспертную комиссию по разрешению спора с привлечением уполномоченных представителей всех участвующих в конкретном инциденте сторон.

12.5.5. Решение Оператора оформляется в форме документа на бумажном носителе по одному экземпляру для каждой стороны с приложением соответствующих первичных документов.

12.5.6. В случае недостижения согласия сторонами спора в досудебном порядке, в том числе в случае несогласия Участника или Оператора УПИ с решением Оператора, привлеченного для разрешения спора, любая из сторон спора вправе обратиться в суд в соответствии с положениями настоящих Правил и заключенных договоров.

12.6. Все споры, разногласия или требования между Оператором и Участниками, Оператором и привлеченными Операторами УПИ, Операторами УПИ и Участниками при недостижении договоренности в досудебном порядке подлежат разрешению в Арбитражном суде г. Москвы.

13. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ПРАВИЛ

13.1. Общие положения

13.1.1. Контроль за соблюдением настоящих Правил Участниками и Операторами УПИ осуществляет Оператор на постоянной основе путем мониторинга деятельности Субъектов в процессе оказания услуг в рамках Платежной системы, анализа жалоб и обращений Отправителей и Получателей, а также Субъектов Платежной системы.

13.1.2. Участники осуществляют контроль за соблюдением настоящих Правил Партнерами, БПА и БПСА в случае их привлечения. За нарушение Партнерами, БПА или БПСА настоящих Правил Участник несет ответственность непосредственно перед Оператором.

13.1.3. Субъекты Платежной системы несут ответственность за любые ненадлежащие действия своих сотрудников (в том числе противоправные), допущенные ими при работе в Платежной системе и повлекшие возникновение ущерба для кого-либо из Субъектов Платежной системы.

13.2. Способы осуществления контроля

13.2.1. Оператор осуществляет контроль за соблюдением Правил следующими способами:

- запрашивает и получает от Субъектов первичную информацию и документы, касающуюся деятельности Субъектов в рамках Системы;
- принимает и рассматривает обращения, поступившие от Клиентов, Участников, Операторов УПИ в отношении действий (бездействий) Участников при оказании услуг;
- осуществляет проверку деятельности Участников в рамках Системы в точках обслуживания Клиентов, в том числе без предварительного уведомления Участников;
- осуществляет действия и применяет меры принуждения в соответствии с настоящими Правилами в случае нарушения Участниками и (или) Операторами УПИ, принятых на себя обязательств в соответствии с настоящими Правилами.

13.3. Действия Оператора при выявлении случаев нарушения Правил

13.3.1. В случаях, если нарушения требований настоящих Правил Субъектами Системы не влияют на БФПС, а также не влияют на услуги, оказываемые Участникам Платежной системы и их Клиентам, Оператор осуществляет следующие действия:

- доводит до сведения Субъекта 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;
- направляет Субъекту рекомендации по устранению выявленного нарушения и рекомендует им представить Оператору программу мероприятий, направленных на устранение нарушения;
- осуществляет контроль за устранением Субъектами выявленного нарушения в установленный в уведомлении срок.

13.3.2. В случаях, если нарушения требований настоящих Правил Субъектами Системы влияют на БФПС либо на услуги, оказываемые Участникам Платежной системы и их Клиентам, Оператор применяет одну из следующих мер принуждения:

- направляет предписание об устранении нарушения с указанием срока для его устранения;
- ограничивает (приостанавливает) оказание операционных услуг и (или) услуг платежного клиринга;
- направляет уведомление о приостановке (прекращении) участия Субъекта в Системе.

13.3.3. Меры принуждения вводятся на основании направляемого Оператором уведомления. Уведомление идентифицирует нарушение и определяет срок, в течение которого нарушение должно быть устранено.

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

14. ОТВЕТСТВЕННОСТЬ ЗА НЕСОБЛЮДЕНИЕ ПРАВИЛ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН

14.1. За неисполнение или ненадлежащее исполнение настоящих Правил, договоров и соглашений, заключенных между Субъектами в рамках деятельности в Системе, Субъекты несут ответственность в порядке и в размере, определенными настоящими Правилами, договорами и соглашениями, а также в соответствии с действующим законодательством Российской Федерации.

14.2. Оператор несет ответственность перед другими Субъектами Системы за прямой документально подтвержденный ущерб вследствие неисполнения Оператором настоящих Правил.

14.3. Упущенная выгода, которая может возникнуть у Субъекта вследствие невыполнения или ненадлежащего выполнения Оператором своих обязательств, возмещению не подлежит. К упущенной выгоде относятся ситуации, связанные с отказом в проведении операции.

14.4. В случае если в результате неисполнения (ненадлежащего исполнения) Оператором своих обязательств образуется просроченная задолженность Оператора перед Участником, Участник вправе требовать от Оператора уплаты неустойки в виде пени. Неустойка начисляется в рублях из расчета 0,01% от суммы задолженности за весь период, начинающийся с календарного дня, следующего за днем, в который такая задолженность подлежала погашению в соответствии с настоящими Правилами, и заканчивающийся в день фактического погашения задолженности.

14.5. Ответственность Оператора за его деятельность в качестве Операционного центра за реальный ущерб, возникший вследствие неоказания (ненадлежащего оказания) операционных услуг Участникам и Расчетному центру ограничена размером разовой неустойки, составляющей 0,01% от суммы неисполненных и(или) исполненных с нарушением срока обязательств, за исключением случаев умышленного неоказания (ненадлежащего оказания) операционных услуг.

14.6. Ответственность Оператора за его деятельность в качестве Платежного клирингового центра за убытки, возникшие вследствие неоказания (ненадлежащего оказания) услуг платежного клиринга Участникам и Расчетному центру, ограничена размером разовой неустойки, составляющей 0,01% от суммы неисполненных и(или) исполненных с нарушением срока обязательств, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежного клиринга.

14.7. Ответственность Расчетного центра перед Участниками наступает в рамках действующего законодательства и договоров банковского счета, заключенных с Участниками. Расчетный центр обязан по требованию Оператора и (или) Участников компенсировать убытки, причиненные им односторонним приостановлением (прекращением) оказания расчетных услуг.

14.8. Участник несет ответственность перед Оператором:

- за несоблюдение настоящих Правил;
- за ущерб, причиненный Участником Оператору;
- за просроченную задолженность перед Оператором и иными Субъектами Системы.

14.9. Если в результате неисполнения (ненадлежащего исполнения) Участником своих обязательств образуется просроченная задолженность по проведению расчетов по операциям, Оператор вправе требовать от Участника уплаты неустойки в виде пени. Неустойка начисляется в рублях из расчета 0,01% от суммы задолженности за весь период, начинающийся с календарного дня, следующего за днем, в который такая задолженность подлежала погашению в соответствии с настоящими Правилами, и заканчивающийся в день фактического погашения задолженности.

14.10. Участник несет ответственность, включая финансовую, перед Субъектами Платежной системы и Клиентами в размере фактически причиненного ущерба.

14.11. Участник несет ответственность перед Расчетным центром в порядке и на условиях, предусмотренных договором банковского счета, заключенного с таким Участником.

14.12. Участник несет ответственность перед Оператором за действия привлеченных Участником третьих лиц, в том числе Партнеров, БПА/БПСА, для чего включает в договоры, заключаемые с третьими лицами, обязательства по исполнению ими требований Правил Платежной системы.

14.13. В случае несоблюдения Участником настоящих Правил Оператор вправе приостановить или прекратить участие Участника в Платежной системе в порядке, предусмотренном пунктом 5.4 Правил.

14.14. В случае нарушения Участником требований по обеспечению защиты информации Оператор вправе потребовать от Участника уплаты штрафа в размере причиненного Оператору и иным Субъектам Системы документально подтвержденного ущерба.

14.15. Субъекты Системы, являющиеся самостоятельными операторами персональных данных, несут ответственность за нарушение условий обработки персональных данных в порядке, предусмотренном действующим законодательством.

14.16. Субъект Системы, поручивший другому Субъекту Системы обработку персональных данных субъектов персональных данных в целях исполнения заключенного договора, вправе требовать от него возмещения реального документально подтвержденного ущерба, понесенного оператором персональных данных в результате нарушения Субъектом Системы, действующим по поручению, условий обработки персональных данных, предусмотренных пунктом 8.1 Правил и Законом №152-ФЗ.

14.17. Субъекты Системы несут ответственность за реализацию системы управления Рисками ИБ в их деятельности в соответствии с требованиями действующего законодательства и Правил. Все Субъекты несут ответственность за управление Рисками ИБ в пределах своих полномочий.

14.18. Субъекты Платежной системы освобождаются от ответственности за неисполнение или ненадлежащее исполнение принятых на себя обязательств при возникновении обстоятельств непреодолимой силы, влияющих на исполнение Сторонами принятых на себя обязательств, возникших вследствие событий чрезвычайного характера, возникших после вступления в силу настоящих Правил, которые невозможно было ни предвидеть, ни предотвратить разумными мерами.

14.19. К обстоятельствам непреодолимой силы относятся события, на которые Субъекты не могут оказывать влияние и за возникновение которых не несут ответственности, например землетрясение, наводнение, стихийные бедствия, пожар, а также забастовка, террористические акты, правительственные постановления или распоряжения государственных органов, военные действия любого характера или срывы в работе системы расчетов между банками и небанковскими кредитными организациями на территории Российской Федерации или за ее пределами, которые препятствуют исполнению Субъектами Платежной системы своих обязательств.

14.20. Сторона, которая не в состоянии выполнить принятые на себя обязательства в силу возникновения обстоятельств непреодолимой силы, обязана немедленно (не позднее следующего рабочего дня) информировать Субъектов, чьи интересы могут быть нарушены, о наступлении таких обстоятельств, сообщить данные о характере обстоятельств, дать оценку их влияния на исполнение своих обязательств и сообщить возможный срок их исполнения. Оператор вправе потребовать от Субъекта подтвердить факт наступления обстоятельств непреодолимой силы официальным письменным документом органа, уполномоченного на выдачу таких документов. Оператор уведомляет других Субъектов Платежной системы о возникновении указанных обстоятельств в течение 1 (одного) рабочего дня с момента ее получения.

15. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПРАВИЛА

15.1. Настоящие Правила могут быть дополнены или изменены в случае появления новых законодательных актов или изменения процессов в Платежной системе, связанных с функционированием Системы.

15.2. Изменения в Правила Системы могут вноситься Оператором в одностороннем порядке либо по соглашению всех сторон Системы.

15.3. Оператор может в одностороннем порядке вносить изменения в Правила Системы, при этом:

15.3.1. До внесения изменений в Правила Оператор обязан обеспечить Участникам возможность предварительного ознакомления с предлагаемыми изменениями и направления своего мнения Оператору в установленный им срок, который не может быть менее одного месяца;

15.3.2. Срок для внесения изменений в Правила должен составлять не менее 1 (одного) месяца со дня окончания срока, указанного в предыдущем подпункте;

15.3.3. Возможность предварительного ознакомления с предлагаемыми изменениями в Правила обеспечивается путем размещения Оператором предлагаемых изменений на сайте Системы;

15.3.4. Субъекты Системы направляют свои предложения по адресу, указанному Оператором на сайте Системы, в срок, указанный в п. 15.3.1 Правил;

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

15.3.6. Субъекты, не направившие уведомления о согласии или несогласии с вносимыми изменениями по указанному Оператором Системы адресу и в срок, указанный Оператором Системы, признаются принявшими предлагаемые изменения Правил Системы;

15.3.7. 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;

15.3.8. Изменения в Правила вступают в силу не менее чем через 1 (один) месяц со дня окончания срока, указанного в п. 15.3.1 Правил. Дата вступления в силу вносимых изменений указывается в Правилах Системы.

15.4. Изменения в Правила Системы по соглашению всех сторон вносятся в следующем порядке:

15.4.1. Оператор на сайте Системы размещает:

- проект Правил Системы или предлагаемые изменения,
- информацию о сроке, в течение которого стороны могут направить Оператору уведомления о согласии или несогласии с вносимыми изменениями,
- адрес, по которому стороны могут направлять уведомления о согласии или несогласии с вносимыми в Правила изменениями;

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

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

15.4.4. Субъекты, не направившие уведомления о согласии или несогласии с вносимыми изменениями по указанному Оператором Системы адресу и в срок, указанный Оператором Системы, признаются принявшими предлагаемые изменения Правил Системы.

15.4.5. 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 Правила вступают в силу с даты, указанной Оператором Системы.

15.4.6. 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.

15.4.7. Согласованную версию Правил Системы с указанием даты вступления изменений в силу Оператор размещает на официальном сайте Системы.

15.5. В случае если Участник не согласен с изменениями Правил, он вправе потребовать расторжения Договора участия, предоставив Оператору не менее чем за 10 (десять) календарных дней до вступления в силу изменений Правил письменное уведомление о расторжении Договора участия. При непредоставлении Участником письменного уведомления о расторжении Договора участия, такие изменения считаются принятыми Участником с момента их вступления в силу. Расторжение Договора участия не освобождает Стороны от исполнения обязательств, возникших до момента его расторжения, в том числе по рассмотрению обращений Клиентов.

15.6. Оператор имеет право в одностороннем порядке вносить изменения в действующие Тарифы, вводить новые Тарифы или увеличивать размера тарифов. Оператор обязан уведомить об этом Банк России в срок не менее чем за 30 (тридцать) календарных дней до дня введения в действие изменений в Правила с предоставлением обоснования указанных изменений. Не является введением новых Тарифов Системы и/или увеличением Тарифов расширение, сокращение списка государств регионов (группы государств, объединенных по каким-либо признакам), указанных в Тарифах, введение возможности осуществления Переводов в иных валютах внутри регионов, направлений, внедрение различных платежных инструментов, способов доставки денежных средств Получателю, изменение суммовых порогов, изменение размера комиссионного вознаграждения, а также изменение любых иных параметров при условии, что изменения, в т.ч. эквивалент иных валют, абсолютные значения комиссионного вознаграждения, не выходят из диапазонов, указанных в отношении определенного региона, направления, способа предоставления Отправителем средств для осуществления Перевода, категории Получателя. При внесении указанных изменений информация доводится до Участников заблаговременно путем размещения информации любым способом, доступным Оператору Системы.

15.7. Оператор обязан представлять в Банк России изменения в Правила не позднее десяти дней со дня внесения соответствующих изменений.

15.8. Оператор обеспечивает доступность редакций Правил Платежной системы, действие которых прекращено, на сайте Оператора.

16. ВЗАИМОДЕЙСТВИЕ С ИНЫМИ ПЛАТЕЖНЫМИ СИСТЕМАМИ

16.1. Платежная система МАРЛИН может осуществлять взаимодействие с другими платежными системами на основании заключенных договоров о взаимодействии операторов платежных систем.

16.2. В рамках взаимодействия с платежными системами Оператор увеличивает перечень предоставляемых Клиентам услуг и/или увеличивает географию предоставления услуг по осуществлению переводов денежных средств.

16.3. Договор о взаимодействии платежных систем может быть заключен при условии отражения порядка взаимодействия в правилах платежных систем.

16.4. Оператор может заключить договор о взаимодействии с оператором иностранной платежной системы при условии отражения порядка взаимодействия в Правилах Платежной системы и правилах иностранной платежной системы.

16.5. На дату утверждения настоящей редакции Правил заключенные договоры с оператором иной платежной системы и(или) с оператором иностранной платежной системы отсутствуют.

Приложение №1 к Правилам Платежной системы МАРЛИН

ФОРМА ЗАЯВЛЕНИЯ НА УЧАСТИЕ В ПЛАТЕЖНОЙ СИСТЕМЕ МАРЛИН

На бланке потенциального Участника

рег. №_____
от «___» _____ 20_ г.

_____
наименование Оператора Платежной системы

_____
адрес Оператора Платежной системы

ЗАЯВЛЕНИЕ
О ПРИСОЕДИНЕНИИ К ПРАВИЛАМ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН

В порядке ст. 428 Гражданского кодекса РФ и ч. 7 ст. 20 Федерального закона от 27.06.2011 «О национальной платежной системе» №161-ФЗ, Заявитель:

Полное наименование организации, присоединяющейся к Правилам Платежной системы МАРЛИН	
Сокращенное наименование организации, присоединяющейся к Правилам Платежной системы МАРЛИН	
Основной государственный регистрационный номер	
Идентификационный номер налогоплательщика	
Адрес местонахождения	
Номер лицензии, иного разрешения на осуществление переводов денежных средств с указанием даты выдачи и органа, его выдавшего	

в лице_____,
(должность и Ф.И.О. уполномоченного представителя Заявителя)

действующего (-ей) на основании _____,
(наименование документа, уполномочивающего представителя Заявителя)

направляет Оператору Платежной системы МАРЛИН (регистрационный номер в реестре операторов платежных систем Банка России №_____) настоящее заявление на участие в Платежной системе МАРЛИН в качестве

☐ Прямого участника ☐ Косвенного участника
(выбрать один из видов участия в Платежной системе МАРЛИН)

для чего Заявитель:

- одновременно с заявлением предоставляет перечень прилагаемых к заявлению документов, определенных Оператором;
- подтверждает, что ознакомился с действующими Правилами Платежной системы МАРЛИН, размещенными на сайте Оператора по адресу: www.marlinpay.ru и заявляет о своем согласии с указанными Правилами;
- представляет соглашение о конфиденциальности.

_____ _____ _____
(должность) *(подпись)* *(инициалы, фамилия)*

М.П. (при наличии)

_____
Ф.И.О., телефон и E-mail контактного лица заявителя, адрес официального сайта заявителя в сети "Интернет"

Приложение №2 к Правилам Платежной системы МАРЛИН

ПРОЕКТЫ ФОРМ ДОГОВОРОВ УЧАСТИЯ В ПЛАТЕЖНОЙ СИСТЕМЕ МАРЛИН

Приложение №2.1. Проект формы Договора участия в Платежной системе для Прямого участника

ДОГОВОР
прямого участия в Платежной системе МАРЛИН

г. _____ «____» _____ 20__ года

Акционерное общество «Марлин», именуемое в дальнейшем **Оператор**, в лице Генерального директора _____, действующего на основании Устава, с одной стороны, и _____, именуемый в дальнейшем **Участник**, в лице _____ _____, действующего на основании _____, с другой стороны, при совместном именовании в дальнейшем Стороны, заключили настоящий договор (далее – «Договор») о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Термины и определения, используемые в Договоре, определены Правилами Платежной системы МАРЛИН (далее – «Правила»).

1.2. Действующая версия Правил и Тарифы Системы размещены на сайте Оператора в сети Интернет по адресу www.marlinpay.ru.

1.3. На основании настоящего Договора Участник вступает в Платежную систему МАРЛИН (далее – «Система») в порядке ст. 428 Гражданского кодекса Российской Федерации и ч. 7 ст. 20 Федерального закона от 27.06.2011 г. «О национальной платежной системе» №161-ФЗ на условиях Правил. Оператор предоставляет Участнику возможность оказывать Услуги Системы в рамках Системы на условиях Правил.

1.4. Заключая настоящий Договор, Участник подтверждает, что ознакомлен и согласен с Правилами, присоединяется к Правилам в целом и обязуется их выполнять.

1.5. Участник признает, что Оператор имеет право в одностороннем порядке вносить изменения в Правила и Тарифы в порядке, установленном Правилами.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Оператор обязан:

2.1.1. Обеспечить Участнику возможность оказания Услуг Системы на условиях Правил посредством:

- обеспечения регистрации Участника в Системе;
- обеспечения технологического и информационного обслуживания Участника;
- организации расчетного обслуживания Участника.

2.1.2. Информировать Участника об изменении Правил, публикуя новую редакцию на официальном сайте Системы в сети Интернет в порядке и сроки, указанные в Правилах.

2.2. Оператор вправе:

2.2.1. Вносить изменения в Правила и контролировать выполнение Правил Участником.

2.2.2. 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 Правил, о данном факте Оператор незамедлительно уведомляет Участника по Согласованным каналам связи.

2.3. Участник обязан:

2.3.1. Самостоятельно организовать финансовое, техническое и технологическое обеспечение оказания Услуг Системы.

2.3.2. Оказывать (в зависимости от вида выбранной Услуги Системы) Услуги Системы в полном соответствии с Правилами.

2.3.3. Поддерживать на Счете, предназначенном для осуществления Участником расчетов в Системе, остаток денежных средств в размере, достаточном для своевременного и полного исполнения своих денежных обязательств при работе в Системе.

2.3.4. Знакомиться и регулярно отслеживать изменения, вносимые в Правила.

2.4. Участник вправе:

2.4.1. Оказывать Услуги Системы в соответствии с Правилами.

2.4.2. Временно приостановить (полностью или частично) оказание Услуг Системы, направив за 10 (Десять) рабочих дней до даты приостановления соответствующее уведомление Оператору по Согласованным каналам связи в соответствии с Правилами.

3. ДОКУМЕНТООБОРОТ

3.1. Порядок и условия организации защищенного электронного документооборота регламентируются Правилами.

3.2. Электронные документы, формируемые Сторонами в соответствии с настоящим Договором, заверенные электронной подписью одной из Сторон, юридически эквивалентны соответствующим документам, выполненным на бумажном носителе, подписанным руководителем (иным уполномоченным представителем) и имеющим оттиск печати данной Стороны, обладают полной юридической силой и являются основанием для возникновения соответствующих прав и обязанностей Сторон, вытекающих из данного электронного документа.

4. ПОРЯДОК ПЛАТЕЖНОГО КЛИРИНГА И РАСЧЕТОВ

4.1. Платежный клиринг по Договору осуществляется на валовой основе в соответствии с Правилами.

4.2. Порядок расчетов регламентируется Правилами.

4.3. Прямой участник предоставляет Расчетному центру Системы право на списание денежных средств со своих Счетов, открытых в данном Расчетном центре. Списание осуществляется на условиях заранее данного Участником акцепта без ограничения по количеству платежных требований, а также по сумме и требованиям из обязательств, вытекающим из участия в Системе при условии, что такое право на списание денежных средств на основании заранее данного акцепта предусмотрено договором банковского (корреспондентского) счета, заключенным между Участником и Расчетным центром.

4.4. Участник приобретает статус Прямого Участника при условии открытия банковских счетов для расчетов в Расчетном центре Системы.

4.5. Расчеты по Договору производятся по реквизитам Участника, информация о которых предоставлена Расчетным центром.

5. ВОЗНАГРАЖДЕНИЕ

5.1. За оказание Услуг Системы в соответствии с Правилами и Тарифами Системы Участник получает и (или) производит выплату вознаграждения, а также оплачивает операционные услуги и услуги платежного клиринга.

5.2. Оплата Участником услуг Расчетного центра по обслуживанию Счета, используемого для работы в Платежной системе, осуществляется в соответствии с договором Участника с Расчетным центром.

6. КОНФИДЕНЦИАЛЬНОСТЬ

6.1. Стороны обязуются сохранять конфиденциальность данных, получаемых при работе в Системе, в т.ч. 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.

6.2. Участники, соглашаются с тем, что осуществляемая Оператором деятельность по сбору и хранению информации, необходимой для функционирования Системы, не нарушает условий конфиденциальности.

6.3. В случае расторжения настоящего Договора 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).

6.4. Обработка персональных данных физических лиц осуществляется в порядке, предусмотренном Правилами, с соблюдением требований действующего законодательства. В случае если в соответствии с условиями Правил для обработки персональных данных физических лиц требуется предоставление поручения на обработку персональных данных другой Стороне, подписанием настоящего Договора Сторона предоставляет такое поручение другой Стороне на условиях, изложенных в Правилах.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Каждая из Сторон самостоятельно отвечает за соблюдение требований применимого законодательства, в т.ч. валютного законодательства, законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма, о защите персональных данных.

7.2. Стороны обязаны гарантировать банковскую тайну.

7.3. Стороны не несут ответственности за полное или частичное неисполнение какого-либо обязательства, если это неисполнение явилось следствием обстоятельств непреодолимой силы, а также вследствие издания законодательных и нормативных актов, обязательных для исполнения Сторонами.

7.4. За неисполнение или ненадлежащее исполнение требований Правил и настоящего Договора, Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации, а также Правилами.

7.5. В случае несоответствия установленному уровню бесперебойности функционирования Платежной системы (БФПС) Участник обязуется возместить Субъектам Платежной системы фактически причиненный им ущерб, подтверждённый документально.

7.6. Уплата штрафных санкций не освобождает нарушившую Сторону от исполнения обязательств по Договору и Правилам.

8. ПРИМЕНИМОЕ ПРАВО И РАССМОТРЕНИЕ СПОРОВ

8.1. Отношения Сторон по настоящему Договору регулируются законодательством Российской Федерации.

8.2. Все споры, которые могут возникнуть между Сторонами в рамках исполнения Договора и/или в связи с ним, подлежат разрешению путем переговоров. Все претензии/сообщения/уведомления в рамках Договора подлежат рассмотрению в порядке, предусмотренном Правилами.

8.3. При невозможности достичь согласия в порядке, предусмотренном п. 8.2. настоящего Договора, споры между Сторонами подлежат рассмотрению в Арбитражном суде г. Москвы.

9. ДЕЙСТВИЕ ДОГОВОРА И ПОРЯДОК ЕГО ПРЕКРАЩЕНИЯ И ИЗМЕНЕНИЯ

9.1. Договор вступает в силу с даты его подписания 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.

9.2. Датой начала участия Участника в Системе является дата подписания Сторонами акта технической готовности, подтверждающего готовность Участника к оказанию Услуг Системы.

9.3. Договор может быть в одностороннем внесудебном порядке изменен и (или) дополнен Оператором Системы, в том числе в случаях внесения изменений в Правила или применимого законодательства, путем заблаговременного направления уведомления о предстоящих изменениях. Уведомление Участника может осуществляться путем размещения информации на сайте Оператора о предстоящих изменениях в Правила. В указанных случаях дополнительное соглашение к Договору может не заключаться, уведомление становится неотъемлемой частью Договора, изменения к Договору вступают в силу с момента, указанного в уведомлении Оператора. В случае несогласия Участника с новыми условиями Договора, Участник вправе прекратить участие в Системе в порядке, предусмотренном Правилами Системы.

9.4. Настоящий Договор может быть изменен и/или дополнен по взаимному согласию Сторон путем заключения дополнительного соглашения к Договору в письменном виде, подписанном уполномоченными представителями Сторон.

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

9.6. 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. Если иное не предусмотрено Правилами, о намерении расторгнуть настоящий Договор заинтересованная Сторона обязана предупредить другую Сторону не позднее, чем за 30 (Тридцать) календарных дней до даты предполагаемого расторжения, и полностью урегулировать финансовые обязательства. Предупреждение о намерении расторгнуть настоящий Договор направляется заинтересованной Стороной в письменном виде с подписями уполномоченных лиц другой Стороне по адресу, указанному в разделе 10 настоящего Договора.

10. ЮРИДИЧЕСКИЕ АДРЕСА И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН

Оператор:	**Участник:**

Приложение №2.2. Проект формы Договора участия в Платежной системе для Косвенного участника

ДОГОВОР
косвенного участия в Платежной системе МАРЛИН

г. _____ «____» _____ 20__ года

Акционерное общество «Марлин», именуемое в дальнейшем «**Оператор**», в лице Генерального директора _____, действующего на основании Устава, с одной стороны, и

_____, именуемый в дальнейшем «**Косвенный участник**», в лице _____ _____, действующего на основании _____, с другой стороны, при совместном именовании в дальнейшем Стороны, заключили настоящий договор (далее – «Договор») о нижеследующем:

1. ПРЕДМЕТ ДОГОВОРА

1.1. Термины и определения, используемые в Договоре, определены Правилами Платежной системы МАРЛИН (далее – «Правила»).

1.2. Действующая версия Правил и Тарифы Системы размещены на сайте Оператора в сети Интернет по адресу www.marlinpay.ru.

1.3. На основании настоящего Договора Косвенный участник вступает в Платежную систему МАРЛИН (далее – «Система») в порядке ст. 428 Гражданского кодекса Российской Федерации и ч. 7 ст. 20 Федерального закона от 27.06.2011 г. «О национальной платежной системе» №161-ФЗ на условиях Правил. Оператор предоставляет Косвенному участнику возможность оказывать Услуги Системы в рамках Системы на условиях Правил.

1.4. Заключая настоящий Договор, Косвенный участник подтверждает, что ознакомлен и согласен с Правилами, присоединяется к Правилам в целом и обязуется их выполнять.

1.5. Косвенный участник признает, что Оператор имеет право в одностороннем порядке вносить изменения в Правила и Тарифы в порядке, установленном Правилами.

2. ПРАВА И ОБЯЗАННОСТИ СТОРОН

2.1. Оператор обязан:

2.1.1. Обеспечить Косвенному участнику возможность оказания Услуг Системы на условиях Правил посредством:

- регистрации Косвенного участника в Системе;
- обеспечения технологического и информационного обслуживания Косвенного участника;
- организации расчетного обслуживания Косвенного участника на условиях, содержащихся в Правилах.

2.1.2. Информировать Косвенного участника об изменении Правил, публикуя новую редакцию на официальном сайте Системы в сети Интернет в порядке и сроки, указанные в Правилах.

2.2. Оператор вправе:

2.2.1. Вносить изменения в Правила и контролировать выполнение Правил Участником.

2.2.2. Без предварительного уведомления Косвенного участника временно приостановить по собственной инициативе полностью или частично работу Косвенного участника в Системе в

случаях неисполнения им своих обязательств в рамках настоящего Договора, а также в случае нарушения Правил, о данном факте Оператор незамедлительно уведомляет Косвенного участника и его Прямого участника по Согласованным каналам связи.

2.3. Косвенный участник обязан:

2.3.1. Самостоятельно организовать финансовое, техническое и технологическое обеспечение оказания Услуг Системы.

2.3.2. Оказывать (в зависимости от вида выбранной Услуги Системы) Услуги Системы в полном соответствии с Правилами.

2.3.3. Поддерживать на Счете, предназначенном для осуществления Косвенными участником расчетов в Системе, остаток денежных средств в размере, достаточном для своевременного и полного исполнения своих денежных обязательств при работе в Системе. В случае, если Косвенный участник не открывает банковский счет у Прямого участника, порядок исполнения денежных обязательств по операциям, совершенным Косвенным участником в Системе, определяется договором между Прямым и Косвенным участником, условия которого не должны противоречить положениям Правил.

2.3.4. Знакомиться и регулярно отслеживать изменения, вносимые в Правила.

2.4. Косвенный участник вправе:

2.4.1. Оказывать Услуги Системы в соответствии с Правилами.

2.4.2. Временно приостановить (полностью или частично) оказание Услуг Системы, направив за 10 (Десять) рабочих дней до даты приостановления соответствующее уведомление Оператору по Согласованным каналам связи в соответствии с Правилами.

3. ДОКУМЕНТООБОРОТ

3.1. Порядок и условия организации защищенного электронного документооборота регламентируются Правилами.

3.2. Электронные документы, формируемые Сторонами в соответствии с настоящим Договором, заверенные электронной подписью одной из Сторон, юридически эквивалентны соответствующим документам, выполненным на бумажном носителе, подписанным руководителем (иным уполномоченным представителем) и имеющим оттиск печати данной Стороны, обладают полной юридической силой и являются основанием для возникновения соответствующих прав и обязанностей Сторон, вытекающих из данного электронного документа.

4. ПОРЯДОК ПЛАТЕЖНОГО КЛИРИНГА И РАСЧЕТОВ

4.1. Платежный клиринг по Договору осуществляется на валовой основе в соответствии с Правилами.

4.2. Порядок расчетов регламентируется Правилами.

4.3. Косвенный участник предоставляет Прямому участнику Системы право на списание денежных средств со своих Счетов, открытых у данного Прямого участника (в случае их открытия). Списание осуществляется на условиях заранее данного Косвенным участником акцепта без ограничения по количеству платежных требований, а также по сумме и требованиям из обязательств, вытекающим из участия в Системе при условии, что такое право на списание денежных средств на основании заранее данного акцепта предусмотрено договором банковского (корреспондентского) счета, заключенным между Косвенным участником и Прямым участником.

4.4. Участник приобретает статус Косвенного участника при условии открытия банковских счетов для расчетов у Прямого участника Системы или заключения с Прямым участником договора об осуществлении взаиморасчетов по операциям, совершенным Косвенным участником в Системе, который не должен противоречить условиям Правил.

4.5. Расчеты по Договору производятся по реквизитам Косвенного участника, информация о которых предоставлена Прямым участником.

5. ВОЗНАГРАЖДЕНИЕ

5.1. За оказание Услуг Системы Косвенный участник получает вознаграждение от Прямого участника и/или производит выплату вознаграждения Прямому участнику, а также оплачивает операционные услуги и услуги платежного клиринга на основании акта участника, направленного Сторонам Оператором в порядке, предусмотренном Правилами. Тарифами Системы могут быть предусмотрены услуги, оплата которых осуществляется Косвенным участником непосредственно Оператору.

5.2. Оплата Косвенным участником услуг Прямого участника по обслуживанию Счета, используемого для работы в Платежной системе, осуществляется в соответствии с договором об открытии (обслуживании) банковского счета.

6. КОНФИДЕНЦИАЛЬНОСТЬ

6.1. Стороны обязуются сохранять конфиденциальность данных, получаемых при работе в Системе, в т.ч. 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 Косвенного участника или условиями, изложенными в Правилах.

6.2. Участники соглашаются с тем, что осуществляемая Оператором деятельность по сбору и хранению информации, необходимой для функционирования Системы, не нарушает условий конфиденциальности.

6.3. В случае расторжения настоящего Договора 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).

6.4. Обработка персональных данных физических лиц осуществляется в порядке, предусмотренном Правилами, с соблюдением требований действующего законодательства. В случае если в соответствии с условиями Правил для обработки персональных данных физических лиц требуется предоставление поручения на обработку персональных данных другой Стороне, подписанием настоящего Договора Сторона предоставляет такое поручение другой Стороне на условиях, изложенных в Правилах.

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. Каждая из Сторон самостоятельно отвечает за соблюдение требований применимого законодательства, в т.ч. валютного законодательства, законодательства о противодействии легализации доходов, полученных преступным путем, и финансированию терроризма, о защите персональных данных.

7.2. Стороны обязаны гарантировать банковскую тайну.

7.3. Стороны не несут ответственности за полное или частичное неисполнение какого-либо обязательства, если это неисполнение явилось следствием обстоятельств непреодолимой силы, а также вследствие издания законодательных и нормативных актов, обязательных для исполнения Сторонами.

7.4. За неисполнение или ненадлежащее исполнение требований Правил и настоящего Договора, Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации, а также Правилами.

7.5. В случае несоответствия установленному уровню бесперебойности функционирования Платежной системы (БФПС) Косвенный участник обязуется возместить Субъектам Платежной системы фактически причиненный им ущерб, подтвержденный документально.

7.6. Уплата штрафных санкций не освобождает нарушившую Сторону от исполнения обязательств по Договору и Правилам.

8. ПРИМЕНИМОЕ ПРАВО И РАССМОТРЕНИЕ СПОРОВ

8.1. Отношения Сторон по настоящему Договору регулируются законодательством Российской Федерации.

8.2. Все споры, которые могут возникнуть между Сторонами в рамках исполнения Договора и/или в связи с ним, подлежат разрешению путем переговоров. Все претензии/сообщения/уведомления в рамках Договора подлежат рассмотрению Стороной в порядке, предусмотренном Правилами.

8.3. При невозможности достичь согласия в порядке, предусмотренном п. 8.2. настоящего Договора, споры между Сторонами подлежат рассмотрению в Арбитражном суде г. Москвы.

9. ДЕЙСТВИЕ ДОГОВОРА И ПОРЯДОК ЕГО ПРЕКРАЩЕНИЯ И ИЗМЕНЕНИЯ

9.1. Договор вступает в силу с даты его подписания 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.

9.2. Датой начала участия Косвенного участника в Системе является дата подписания Сторонами акта технической готовности, подтверждающего готовность Косвенного участника к оказанию Услуг Системы.

9.3. Договор может быть в одностороннем внесудебном порядке изменен и (или) дополнен Оператором Системы, в том числе в случаях внесения изменений в Правила или применимого законодательства, путем заблаговременного направления уведомления о предстоящих изменениях. Уведомление Косвенного участника может осуществляться путем размещения информации на сайте Оператора о предстоящих изменениях в Правила. В указанных случаях дополнительное соглашение к Договору может не заключаться, уведомление становится неотъемлемой частью Договора, изменения к Договору вступают в силу с момента, указанного в уведомлении Оператора. В случае несогласия Косвенного участника с новыми условиями Договора, Косвенный участник вправе прекратить участие в Системе в порядке, предусмотренном Правилами Системы.

9.4. Настоящий Договор может быть изменен и/или дополнен по взаимному согласию Сторон путем заключения дополнительного соглашения к Договору в письменном виде, подписанном уполномоченными представителями Сторон.

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

9.6. 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. Если иное не предусмотрено Правилами, о намерении расторгнуть настоящий Договор заинтересованная Сторона обязана предупредить другую Сторону не позднее, чем за 30 (Тридцать) календарных дней до даты предполагаемого расторжения, и полностью урегулировать финансовые обязательства. Предупреждение о намерении расторгнуть настоящий Договор направляется заинтересованной Стороной в письменном виде с подписями уполномоченных лиц другой Стороне по адресу, указанному в разделе 10 настоящего Договора.

10. ЮРИДИЧЕСКИЕ АДРЕСА И БАНКОВСКИЕ РЕКВИЗИТЫ СТОРОН

Оператор:	Косвенный участник:

Приложение №3 к Правилам Платежной системы МАРЛИН

ТАРИФЫ

Платежной системы МАРЛИН

Категория перевода денежных средств	Тип операции	Тарифы для Отправителей[1]	Тарифы для Участников[2]
Переводы в пределах Российской Федерации	Отправка переводов денежных средств по территории Российской Федерации	От 0% до 6% от суммы перевода денежных средств; и/или фиксированная сумма от 0 рублей до 2000 рублей	От 0% до 45% от суммы комиссии, уплачиваемой Отправителем в соответствии с Тарифами для Отправителей; и/или от 0% до 1% от суммы перевода денежных средств; и/или фиксированная сумма от 0 рублей до 750 рублей.
	Выплата переводов денежных средств по территории Российской Федерации	Плата не взимается	От 0% до 35 % от суммы комиссии, уплачиваемой Отправителем в соответствии с Тарифами для Отправителей; и/или от 0% до 1% от суммы перевода денежных средств; и/или фиксированная сумма от 0 рублей до 750 рублей.
Трансграничные Переводы	Отправка переводов денежных средств из Российской Федерации	От 0% до 6% от суммы перевода денежных средств; и/или фиксированная сумма от 0 рублей/долларов США/ ЕВРО до 6000 рублей/300 долларов США/300 ЕВРО	От 0% до 45 % от суммы комиссии, уплачиваемой Отправителем в соответствии с Тарифами для Отправителей; и/или от 0% до 1,5% от суммы перевода денежных средств и/или фиксированная сумма от 0 рублей/долларов США/ ЕВРО до 3000 рублей/150 долларов США/ЕВРО
	Выплата переводов денежных средств	Плата не взимается	От 0% до 45 % от суммы комиссии, уплачиваемой Отправителем в соответствии с Тарифами для Отправителей; и/или от 0% до 1,5% от суммы перевода денежных средств и/или фиксированная сумма от 0 рублей/долларов США/ ЕВРО до 3000 рублей/150 долларов США/ЕВРО
Оплата в пользу юридических лиц и индивидуальных предпринимателей за товары, работы, услуги	- от физических лиц с целью увеличения остатка электронных денежных средств - от физических лиц для зачисления на счета/карты физических лиц в кредитных	От 0% до 30% от суммы перевода денежных средств; и/или фиксированная сумма от 0 до 2000 рублей	От 0% до 75% от суммы комиссии, уплачиваемой Отправителем в соответствии с Тарифами для Отправителей; и/или от 0% до 20% от суммы перевода денежных средств; и/или фиксированная сумма от 0

[1] Информация о конкретном размере комиссионного вознаграждения, взимаемого с Отправителя за осуществление перевода денежных средств размещается на официальном сайте Платежной системы, а также доводится до сведения Отправителя до момента осуществления перевода денежных средств в местах обслуживания клиентов Участников или привлеченных ими лиц, в т.ч. на дисплеях терминалов самообслуживания, с помощью систем ДБО

[2] Информация о конкретном размере вознаграждения Участников определяется Оператором Системы, фиксируется в ПО Системы.

	организациях, в том числе Переводы на карты международных и национальных платежных систем - от физических лиц юридическим лицам и индивидуальным предпринимателям при предоставлении реквизитов платежа - от физических лиц в оплату товаров, работ и услуг, предоставляемых юридическими лицами и индивидуальными предпринимателями		до 600 рублей

Приложение №4 к Правилам Платежной системы МАРЛИН

ПОЛОЖЕНИЕ ПО УПРАВЛЕНИЮ ИНЦИДЕНТАМИ, СВЯЗАННЫМИ С НАРУШЕНИЕМ ТРЕБОВАНИЙ К ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ОСУЩЕСТВЛЕНИИ ПЕРЕВОДОВ ДЕНЕЖНЫХ СРЕДСТВ В ПЛАТЕЖНОЙ СИСТЕМЕ МАРЛИН

1. Общие положения

1.1. Настоящее Положение рассматривает следующие вопросы:

- обнаружение, оповещение Субъектов Платежной системы об инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе с применением СКЗИ;
- реагирование на инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, включая активизацию соответствующих защитных мер, а также регистрация инцидентов;
- анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

1.2. Настоящее Положение обязательно для применения всеми структурными подразделениями Оператора Платежной системы, а также всеми Субъектами Платежной системы МАРЛИН.

2. Термины и определения

Инциденты[1] **–** события, которые возникли вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств и (или) условий осуществления (требований к осуществлению) перевода денежных средств, связанных с обеспечением защиты информации при осуществлении переводов денежных средств, в том числе включенных в перечень типов инцидентов, согласованный с федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и размещаемый Банком России на официальном сайте Банка России в сети Интернет, которые:

- привели к несвоевременности осуществления переводов денежных средств (к нарушению сроков, установленных законодательством Российской Федерации, Правилами Платежной системы и (или) договорами, заключаемыми Клиентами, Операторами УПИ, Оператором, Участниками и привлеченными ими лицами);
- привели или могут привести к осуществлению переводов денежных средств по распоряжению лиц, не обладающих правом распоряжения этими денежными средствами;
- привели к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в распоряжениях Клиентов, Распоряжениях Участников Платежной системы, распоряжениях Платежного клирингового центра.

Причинами возникновения Инцидентов могут являться:

- воздействие вредоносного кода, приводящее к нарушению штатного функционирования средства вычислительной техники, СКЗИ, результатом которого является нарушение предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств;

[1] Термин применяется к инцидентам информационной безопасности.

- реализация воздействий на автоматизированные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, эксплуатация которых обеспечивается Операторами УПИ, Участниками и привлеченными ими лицами, и используется для осуществления переводов денежных средств (далее - объекты информационной инфраструктуры), с целью создания условий невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств;
- нарушение конфиденциальности информации, необходимой для удостоверения Клиентами операторов по переводу денежных средств права распоряжения денежными средствами;
- компрометация ключевой информации СКЗИ, используемых при осуществлении переводов денежных средств;
- осуществление переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, вследствие нарушения конфиденциальности информации, необходимой для удостоверения Клиентами операторов по переводу денежных средств права распоряжения денежными средствами или вследствие компрометации ключевой информации СКЗИ, используемых при осуществлении переводов денежных средств;
- воздействие вредоносного кода, приводящее к осуществлению переводов денежных средств с использованием искаженной информации, содержащейся в Распоряжениях Клиентов, оформленных в рамках применяемой формы безналичных расчетов, Распоряжениях Участников, Распоряжениях Платежного клирингового центра;
- невозможность предоставления услуг по переводу денежных средств в Платежной системе в полном объеме в течение шести часов и более;
- списание денежных средств без добровольного согласия Участников с банковских счетов Участников, в том числе с использованием искаженной информации, содержащихся в Распоряжениях Участников.

Иные термины и определения, содержащиеся в настоящем Положении, трактуются в соответствии с Правилами Платежной системы МАРЛИН.

3. Обнаружение Инцидентов, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств

3.1. Инцидентами, связанными с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, считаются события, ставшие последствиями реализации рисков нарушения требований к защите информации при осуществлении переводов денежных средств.

3.2. Источниками информации об Инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе, могут быть:

- сообщения работников структурного подразделения по защите информации;
- сообщения работников других структурных подразделений;
- сведения, отраженные в журналах регистрации событий информационных систем;
- результаты работы средств защиты информации;
- результаты внутренних проверок;
- обращения Субъектов Платежной системы с указанием Инцидента, связанного с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- уведомления и сообщения Банка России и иных регулирующих органов в пределах своих полномочий;

– другие источники информации.

3.3. Работник Оператора или иного Субъекта Платежной системы может выявить признаки наличия Инцидента, связанного с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, путем анализа текущей ситуации на предмет ее соответствия требованиям Правил, а также на предмет реализации рисков нарушения требований к обеспечению защиты информации. Выявленные несоответствия дают основания предполагать факт возникновения Инцидента, связанного с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств. Любые сведения об Инцидентах, должны быть незамедлительно переданы выявившим их работником лицу, ответственному за взаимодействие с Оператором по вопросам выявления и предотвращения Инцидентов (далее – ответственное лицо):

– по контактам, указанным во внутрикорпоративном справочнике;

– через непосредственного руководителя работника.

3.4. В случае подтверждения факта возникновения Инцидента, ответственное лицо Субъекта информирует о возникновении Инцидента других Субъектов в соответствии с порядком, установленным в настоящем Положении.

3.5. Все Участники Платежной системы и Операторы УПИ на этапе заключения договорных отношений назначают лиц, ответственных за взаимодействие с Оператором по вопросам выявления и предотвращения Инцидентов в Платежной системе и предоставляют Оператору их контактные данные в рамках Согласованных каналов связи.

3.6. Участники Платежной системы и Операторы УПИ, а также Оператор обязаны своевременно сообщать об изменении предоставленных контактных данных.

4. Регулярное информирование об Инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств

4.1. Ответственные лица Участников Платежной системы, а также Операторов УПИ обеспечивают ежемесячное информирование Оператора Платежной системы о выявленных Инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе.

4.2. Информация о выявленных Инцидентах, связанных с нарушениями требований к обеспечению защиты информации, должна ежемесячно предоставляться Оператору ответственными лицами Участников Платежной системы и Операторов УПИ не позднее 5 (пятого) рабочего дня месяца, следующего за отчетным, и подтверждаться письменно путем предоставления Отчета о выявленных Инцидентах, связанных с нарушениями требований к обеспечению защиты информации. Отчет предоставляется в свободной форме с указанием количества Инцидентов за отчетный месяц и дат их возникновения/выявления (п. 2.3 Приложения №5).

4.3. При отсутствии Инцидентов за соответствующий период Участники Платежной системы и Операторы УПИ направляют Оператору Платежной системы отчет, содержащий нулевые данные.

4.4. Информирование Оператора о выявленных Инцидентах осуществляется путем направления официальных писем в адрес Оператора с дублированием соответствующих сообщений по Согласованным каналам связи в адрес ответственного лица Оператора. При необходимости оперативного реагирования на выявленный Инцидент информирование Оператора Платежной системы о выявленных Инцидентах осуществляется посредством телефонной связи.

4.5. Оператор предоставляет информационное сообщение о выявленных в Платежной системе Инцидентах Участникам и Операторам УПИ в ЛК или по Согласованным каналам связи ежемесячно, не позднее двенадцати рабочих дней, следующих за отчетным месяцем.

4.6. При необходимости оповещения Оператором других субъектов о выявленных в Платежной системе Инцидентах, связанных с нарушением требований к обеспечению защиты информации при

осуществлении переводов денежных средств, информирование может осуществляться по Согласованным каналам связи с ответственными лицами субъектов.

4.7. Оператор обеспечивает учет и доступность для Участников и Операторов УПИ информации о выявленных в Платежной системе Инцидентах, связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в порядке, предусмотренном пунктом 10.2.24 Правил.

5. Порядок оперативного взаимодействия Оператора с Участниками и Операторами УПИ в случае выявления в Платежной системе Инцидентов

5.1. Субъект при выявлении в Платежной системе Инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, принимает необходимые меры по снижению негативных последствий, вызванных нарушением требований, и незамедлительно, в течение 24 часов с момента наступления событий, информирует ответственное лицо Оператора путем направления по Согласованным каналам связи уведомления по форме, предусмотренной Приложением А к настоящему Положению по управлению инцидентами, связанными с нарушением требования к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе МАРЛИН. Оператор проводит анализ предоставленных данных, в случае подтверждения реализует комплекс мер, направленных на устранение последствий Инцидента, причин, вызвавших Инцидент, и на недопущение его повторного возникновения, при необходимости направляет соответствующее уведомление тому Субъекту ПС, в функциональной зоне ответственности которого находится область возникновения Инцидента для принятия незамедлительных мер.

5.2. Субъект, допустивший Инцидент, реализует комплекс мер, направленных на восстановление штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации, а также на устранение последствий Инцидента, причин, вызвавших Инцидент, и на недопущение его повторного возникновения.

5.3. Для восстановления штатного функционирования объекта информационной инфраструктуры в случае реализации инцидентов защиты информации Субъект должен иметь внутренние документы по восстановлению штатного функционирования объектов информационной инфраструктуры, которые должны предусматривать последовательные действия, направленные на восстановление работоспособности вышедших из строя автоматизированных систем и(или) программного обеспечения в зависимости от причин возникновения Инцидента, и в случае реализации Инцидента действовать в соответствии с ними.

5.4. Оператор определяет следующие требования к мероприятиям по восстановлению штатного функционирования объектов информационной инфраструктуры операторов по переводу денежных средств, являющихся Участниками Системы, и Операторов УПИ, которые должны обеспечивать непрерывность работы в нештатных ситуациях:

- поддержание актуального перечня объектов информационной инфраструктуры, используемого для работы в Платежной системе;
- наличие резервного оборудования, каналов связи, резервных копий программного обеспечения, средств защиты информации, используемых Субъектом для работы в Платежной системе;
- регулярное выполнение процедур резервного копирования операций, осуществленных в Платежной системе, с применением средств защиты информации;
- наличие конкретных восстановительных решений для соответствующего типа объекта информационной инфраструктуры в зависимости от причины возникновения Инцидента;
- предотвращение возникновения нештатных ситуаций в будущем путем поиска и устранения выявленных ошибок функционирования объектов информационной инфраструктуры, а также путем оптимизации используемых объектов информационной инфраструктуры;

- обеспечение корректировки рабочей документации на используемые объекты информационной инфраструктуры по результатам проведения анализа возникновения нештатных ситуаций и перечня мероприятий для недопущения повторения нештатных ситуаций в будущем;
- регулярное обучение персонала.

Для минимизации времени восстановления объектов информационной инфраструктуры, используемого операторами по переводу денежных средств, являющихся Участниками, и Операторами УПИ, для работы в Платежной системе должно быть обеспечено выполнение требований по:

- управлению порядком функционирования и восстановления объектов информационной инфраструктуры;
- определению критически значимых объектов информационной инфраструктуры, используемых для работы в Платежной системе;
- резервированию критически значимых объектов информационной инфраструктуры,
- контролю работоспособности резервных объектов информационной инфраструктуры;
- техническому обслуживанию объектов информационной инфраструктуры, используемых для работы в Платежной системе, на постоянной основе (комплекс работ по поддержанию технических средств в работоспособном состоянии);
- организации дежурства специалистов по техническому сопровождению (при необходимости).

5.5. Субъект должен регулярно, но не реже одного раза в два года, тестировать мероприятия, предусмотренные внутренними документами Субъектов, разработанных с учетом требований Оператора, установленных в настоящем разделе Приложения, направленные на восстановление штатного функционирования объектов информационной инфраструктуры, прерывание функционирования которых вызвано Инцидентами.

5.6. В случае, если для устранения последствий выявленного Инцидента, связанного с нарушением требований к обеспечению защиты информации при осуществлении перевода денежных средств, у Субъектов возникает необходимость привлечения других Субъектов, то ответственные лица Субъекта, выявившего Инцидент, вправе обратиться к ответственному лицу Оператора для организации взаимодействия в целях устранения последствий выявленного Инцидента.

5.7. При принятии совместных действий по устранению последствий выявленных Инцидентов, ответственные лица Субъектов ставят в известность ответственное лицо Оператора о предпринятых действиях и их результатах.

5.8. В случае выявления Инцидента, для устранения последствий которого необходимо привлечение Оператора, Участник или Оператор УПИ информирует Оператора о данном Инциденте и о том, что для устранения последствий Инцидента требуется его участие. Оператор информирует Участника или Оператора УПИ аналогичным образом в случае выявления им Инцидента, для устранения последствий которого требуется их привлечение.

5.9. Оператор определяет следующий порядок взаимодействия Субъектов Платежной системы при выявлении Инцидентов, возникших вследствие следующих причин.

№ п/п	Причина Инцидента	Действия Субъектов Платежной системы
1.	Воздействие вредоносного кода	В случае наличия опасности распространения последствий воздействия вредоносного кода Субъект, выявивший Инцидент: 1. прекращает информационный обмен в электронном виде с другими Субъектами;

		2. незамедлительно информирует Оператора о возникшей ситуации, в том числе о событиях, по его мнению, вызвавших указанный Инцидент, его причинах и последствиях посредством любого из доступных каналов связи (телефону, электронной почте и т.д.); 3. проводит работы по восстановлению штатного функционирования объектов информационной инфраструктуры, используемых для работы в Платежной системе в соответствии внутренними документами, разработанными в соответствии с требованиями Оператора, предусмотренными пп. 5.2-5.5 настоящего Приложения. Оператор при необходимости информирует других Субъектов о возникновении Инцидента и возможности распространения его последствий. Ответственное лицо Субъекта, выявившего Инцидент, информирует стороны информационного обмена о возобновлении указанного вида информационного обмена после устранения последствий воздействия вредоносного кода.
2	Умышленное или неумышленное нарушение работником Субъекта порядка эксплуатации объекта информационной инфраструктуры Сбой и (или) отказ в работе объектов информационной инфраструктуры, за исключением банкоматов, платежных терминалов, электронных терминалов Сбой и (или) отказ в работе СКЗИ Физическое воздействие на объект информационной инфраструктуры, за исключением банкомата, платежного терминала, электронного терминала, приводящее к повреждению данного объекта информационной инфраструктуры Хищение объекта информационной инфраструктуры, за исключением банкомата, платежного терминала, электронного терминала	Субъект, выявивший Инцидент: 1. при необходимости в оперативном порядке информирует Оператора о наступлении Инцидента с указанием его описания, причин возникновения и последствий; 2. проводит работы по восстановлению штатного функционирования объектов информационной инфраструктуры, используемых для работы в Платежной системе в соответствии внутренними документами, например, разработанными в соответствии с требованиями Оператора, предусмотренными пп. 5.2 - 5.5 настоящего Приложения. Ответственное лицо Оператора при получении информации об Инциденте/выявлении Инцидента вправе принимать решение о необходимости блокировки Субъектов, аннулировании переводов, а также иные решения, направленные на устранение последствий Инцидента. О принятых решениях, а также об их отмене сообщается ответственным лицам Субъектов по Согласованным каналам связи.

3.	Использование электронного средства платежа без добровольного согласия Клиента вследствие противоправных действий, потери, нарушения конфиденциальности информации, необходимой для удостоверения Клиентами оператора по переводу денежных средств права распоряжения денежными средствами	Оператор по переводу денежных средств, получивший информацию об Инциденте, в оперативном порядке информирует ответственное лицо Оператора по Согласованным каналам связи о наступлении Инцидента с указанием его описания, последствий и причин возникновения. Ответственное лицо Оператора при получении информации об Инциденте/выявлении Инцидента вправе признать недействительными неправомерно осуществленные переводы денежных средств в Платежной системе.
	Выявление в совершаемой операции признаков, характерных для операций без добровольного согласия Клиента	
	Размещение на банкоматах и платежных терминалах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств, в том числе аутентификационной информации	
	Распространение информации, побуждающей Клиента оператора по переводу денежных средств сообщать информацию, необходимую для осуществления переводов денежных средств от его имени, в том числе аутентификационную информацию	
4.	Внешнее воздействие из сети Интернет	Ответственное лицо Оператора при получении информации об Инциденте/выявлении Инцидента вправе временно приостановить работу Участника и/или расчеты с Оператором УПИ. Участник или Оператор УПИ обеспечивает восстановление штатного функционирования объектов информационной инфраструктуры, используемых для работы в Платежной системе в соответствии внутренними документами, разработанными в соответствии с требованиями Оператора, предусмотренными пп. 5.2-5.5 настоящего Приложения. О принятых решениях, а также об их отмене сообщается ответственным лицам Участников и (или) Операторам УПИ по Согласованным каналам связи.

6. Порядок анализа и реагирования на Инциденты, связанные с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств

6.1. Ответственное лицо Субъекта после получения информации о выявленном Инциденте незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа ответственное лицо проводит проверку наличия в выявленном факте нарушений работников и анализ обстоятельств, приведших к возникновению Инцидента.

6.2. По результатам анализа причин и последствий Инцидента ответственное лицо по согласованию с непосредственным руководителем в максимально короткие сроки определяет и инициирует первоочередные меры, направленные на локализацию Инцидента и на минимизацию его последствий.

6.3. В процессе проведения мероприятий по устранению последствий Инцидента ответственным лицом Субъекта должны быть установлены следующие факты:

– дата и время совершения /возникновения Инцидента;

– тип Инцидента;

– условия и причина возникновения Инцидента;

– вид нарушителя, виновного в совершении Инцидента (внутренний/внешний);

– обстоятельства и мотивы совершения Инцидента;

– требования по обеспечению защиты информации, вследствие нарушения которых возник Инцидент;

– последствия Инцидента;

– действия, необходимые для устранения последствий Инцидента;

– факт обращения в правоохранительные органы;

– планируемая дата завершения разбирательства по Инциденту.

6.4. По итогам рассмотрения всех сведений об Инциденте ответственным лицом Субъекта должно быть принято решение о целесообразности применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для нейтрализации последствий Инцидентов.

6.5. По результатам расследования Инцидента ответственное лицо формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение, включающее установленные факты об Инциденте, принятые меры по нейтрализации последствий Инцидента и иные обстоятельства, имеющие отношения к устранению последствий Инцидента.

6.6. В случае выявления в Инциденте признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, ответственное лицо передает все материалы по Инциденту в юридическую службу Субъекта для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

6.7. На заключительном этапе устранения последствий Инцидента ответственное лицо проводит анализ результатов реагирования на Инцидент с целью определения достаточности принятых мер.

6.8. По завершению мероприятий, направленных на устранение последствий Инцидента, ответственное лицо проводит итоговый анализ причин возникновения Инцидента. Целью такого анализа является выработка организационных и технических решений, направленных на предотвращение и минимизацию последствий возможных нарушений в будущем. В рамках такого анализа ответственное лицо может проводить следующие мероприятия:

- переоценка рисков, повлекших возникновение Инцидента;
- подготовка перечня защитных мер для минимизации выявленных рисков в случае повторения Инцидента;
- актуализация внутренних документов Субъекта, затрагивающих вопросы обеспечения защиты информации при осуществлении переводов денежных средств;
- проведение обучения персонала Субъекта.

6.9. Субъекты осуществляют регистрацию Инцидентов в соответствии с внутренним порядком, установленным Субъектом. Хранение сведений об Инцидентах осуществляется в порядке, предусмотренном действующим законодательством и нормативными актами Банка России.

6.10. Субъекты по окончании разбора Инцидента направляют Оператору по Согласованным каналам связи заполненную форму, предусмотренной Приложением А к настоящему Положению по управлению Инцидентами, связанными с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе МАРЛИН.

Приложение А

к Положению по управлению Инцидентами, связанными с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе МАРЛИН

Форма оперативного информирования Оператора Субъектами о выявленных в Платежной системе МАРЛИН Инцидентах[1]

N п/п	Сведения по Инциденту	Описание
1	Наименование Субъекта, статус Субъекта, номер и дата договора с Оператором Платежной системы МАРЛИН	
2	Время и дата возникновения Инцидента (в случае невозможности установить время возникновения Инцидента указывается время его выявления)	
3	Краткое описание Инцидента (характеристика произошедшего события и его последствия)	
4	Перечень СКЗИ	
5	Нарушенное требование по обеспечению защиты информации	
6	Мероприятия по устранению Инцидента и его неблагоприятных последствий с указанием планируемой и фактической продолжительности проведения данных мероприятий	
7	Факт обращения в правоохранительные органы	
8	Сведения о выявлении Инцидента Клиентом, Партнером, БПА/БПСА, операционным центром, находящимся за пределами Российской Федерации	
9	Наименование Партнера, БПА/БПСА	
10	Дата завершения разбирательства по Инциденту	

[1] При первичном направлении указанной формы в порядке, предусмотренном п. 5.1 настоящего Положения, Субъект заполняет те данные, которые ему известны на момент направления формы Оператору. При повторном направлении формы в порядке, предусмотренном п. 6.10 Положения, Субъект заполняет форму полностью.

Приложение №5 к Правилам Платежной системы МАРЛИН

ПОРЯДОК ИНФОРМИРОВАНИЯ ОПЕРАТОРА ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН ОБ ОБЕСПЕЧЕНИИ ЗАЩИТЫ ИНФОРМАЦИИ

1. Общие положения

1.1. Настоящий Порядок устанавливает требования к содержанию, форме и периодичности представления информации, направляемой Субъектами Оператору для целей анализа обеспечения в Платежной системе защиты информации при осуществлении переводов денежных средств.

1.2. Информация, направляемая Оператору Участниками и Операторами УПИ для целей анализа предпринимаемых мер, направленных на обеспечение защиты информации при осуществлении переводов денежных средств в Платежной системе, включает:

- сведения о выполнении требований к обеспечению защиты информации;
- сведения о результатах проведенных оценок соответствия;
- сведения о реализации порядка обеспечения защиты информации;
- сведения о выявленных инцидентах (событиях), связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе с применением СКЗИ;
- отчет о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации в Платежной системе;
- список используемых СКЗИ для обеспечения защиты информации в Платежной системе;
- внутренние документы или выписки из них, отражающие порядок действий по восстановлению штатного функционирования объектов информационной инфраструктуры, используемых при работе в Платежной системе, в случае реализации инцидента информационной безопасности и (или) результаты тестирования, указанных мероприятий (например, План ОНиВД).

2. Содержание, форма и сроки предоставления информации

2.1. Участники и Операторы УПИ в свободной форме предоставляют Оператору сведения о результатах проведенных оценок соответствия, о выполнении требований к обеспечению защиты информации и о реализации порядка обеспечения защиты информации. Сведения предоставляются по запросу Оператора Системы в течение 10 рабочих дней, но не реже 1 (одного) раза в 2 (два) года.

2.2. Участники и Операторы УПИ предоставляют Оператору сведения о выявленных инцидентах (событиях), связанных с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств, в том числе с применением СКЗИ. Направляемая Оператору информация должна содержать сведения о самостоятельно выявленных потенциальных угрозах и уязвимостях, касающихся нарушения организационных и (или) технических требований в обеспечении защиты информации при осуществлении переводов денежных средств в Платежной системе. Сведения направляются в порядке и сроки, предусмотренные разделом 3, 5 и 6 Положения по управлению инцидентами, связанными с нарушением требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной системе МАРЛИН (Приложение №4 к Правилам).

2.3. Участники и Операторы УПИ составляют и предоставляют Оператору отчет о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств. Отчет предоставляется в свободной форме при выявлении инцидентов в сфере защиты информации вне зависимости от оперативного информирования Оператора Системы с указанием количества инцидентов за отчетный месяц, дат их возникновения/выявления. При отсутствии инцидентов за отчетный период предоставляется отчет с нулевыми данными. Отчет предоставляется не позднее 5 (пятого) рабочего дня месяца, следующего за отчетным, а также по запросу Оператора.

2.4. Участники и Операторы УПИ предоставляют Оператору сведения о наименовании СКЗИ, номере версии и номере сертификата соответствия ФСБ, используемых ими для обеспечения защиты информации в Платежной системе. Сведения, предусмотренные настоящим пунктом, предоставляются при подключении Субъекта к Платежной системе МАРЛИН, а также по запросу Оператора Системы в течение 10 (десяти) рабочих дней, но не реже 1 (одного) раза в 2 (два) года.

2.5. Участники и Операторы УПИ предоставляют Оператору внутренние документы или выписки из них, которые должны содержать порядок действий Субъекта по восстановлению штатного функционирования объектов информационной инфраструктуры, используемых Субъектом при работе в Платежной системе, в случае реализации инцидента информационной безопасности и (или) результаты тестирования указанных мероприятий (например, План ОНиВД). Сведения, предусмотренные настоящим пунктом, предоставляются по запросу Оператора Системы в течение 10 (десяти) рабочих дней, но не реже 1 (одного) раза в 2 (два) года.

2.6. Указанные сведения предоставляются Участниками и Операторами УПИ в электронном виде по Согласованным каналам связи в адрес ответственного лица Оператора.

2.7. Получаемую информацию ответственное лицо по информационной безопасности Оператора анализирует на предмет обеспечения в Платежной системе достаточного уровня защиты информации, формулирует при необходимости рекомендации по совершенствованию процессов защиты информации, а также на основании анализа вносит изменения в определяемые Оператором требования по защите информации. Оператор информирует Участников и Операторов УПИ обо всех изменениях, касающихся требований по защите информации в Платежной системе.

Приложение №6 к Правилам Платежной системы МАРЛИН

СОСТАВ И ПОРОГОВЫЕ ЗНАЧЕНИЯ ПОКАЗАТЕЛЕЙ УРОВНЯ РИСКА ИБ УЧАСТНИКА ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН

Типы событий/инцидентов нарушений защиты информации	Состав показателей уровня Риска ИБ Участника Платежной системы МАРЛИН	Пороговые значения показателей уровня Риска ИБ Участника Платежной системы МАРЛИН
Инциденты ИБ, за исключением Инцидентов нарушения информационной безопасности Участника, связанных с совершением операций без добровольного согласия клиентов	Количество Инцидентов нарушения информационной безопасности Участника в Системе	Не более 2-х в месяц
	Размер убытков от Инцидентов Риска ИБ Участника, понесенных Оператором Системы	Более 500 000 рублей за 2 месяца
События нарушения информационной безопасности Участника в Системе, связанные с совершением операций без добровольного согласия клиентов	Количество операций, соответствующих признакам осуществления перевода денежных средств без добровольного согласия клиента - физического лица, по которым Участник не приостановил прием к исполнению распоряжения или не отказал в исполнении распоряжения в нарушение требований, предусмотренных п. 10.6.7 Правил.	Не более 2-х в месяц
	Отношение количества операций, соответствующих признакам осуществления перевода денежных средств без добровольного согласия клиента - физического лица, за календарный месяц к среднеарифметическому количеству операций, соответствующих признакам осуществления перевода денежных средств без добровольного согласия клиента - физического лица, за предыдущий квартал	Более 50%

Ограничения по параметрам операций по осуществлению переводов денежных средств в случае выявления факта превышения пороговых значений показателей уровня Риска ИБ Участника Платежной системы МАРЛИН

	Участники, являющиеся операторами по переводу денежных средств	Оператор УПИ
Условия применения ограничений	Оператором Системы могут быть введены ограничения на сумму	Оператором Системы могут быть введены ограничения на сумму

	единичной операции по переводу денежных средств Оператором Платежной системы могут быть введены ограничения на временной период совершения операций	единичной операции по переводу денежных средств Оператором Платежной системы могут быть введены ограничения на временной период совершения операций
Условия снятия ограничений	отсутствие инцидентов защиты информации в течение 3 (трех) месяцев, следующих за месяцем применения ограничений; предоставлены документы и информация об устранении причин возникновения инцидентов защиты информации; возмещены убытки, причиненные Оператору Системы оператором по переводу денежных средств, являющимся Участником Системы.	отсутствие инцидентов защиты информации в течение 3 (трех) месяцев, следующих за месяцем применения ограничений; предоставлены документы и информация об устранении причин возникновения инцидентов защиты информации; возмещены убытки, причиненные Оператору Системы Оператором УПИ.

Приложение №7 к Правилам Платежной системы МАРЛИН

ФОРМА ИНФОРМИРОВАНИЯ СУБЪЕКТОМ ОПЕРАТОРА О ВЫЯВЛЕННЫХ В ПЛАТЕЖНОЙ СИСТЕМЕ ИНЦИДЕНТАХ

N п/п	Сведения по инциденту	Описание
1	Наименование и статус Субъекта Платежной системы МАРЛИН	
2	Дата и время возникновения/выявления инцидента	
3	Краткое описание инцидента (характеристика и последствия)	
4	Наименование одного или нескольких бизнес-процессов, в ходе которых произошел инцидент	
5	Наименование одного или нескольких бизнес-процессов, на которые оказал влияние инцидент	
6 *	Наличие (отсутствие) факта приостановления (прекращения) оказания УПИ в результате инцидента	
7 **	Влияние инцидента на БФПС	
8 **	Степень влияния инцидента на функционирование Платежной системы в зависимости от количества Операторов УПИ, и (или) количества и значимости Участников, на которых оказало непосредственное влияние инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных Распоряжений Участников, и иных факторов	
9 *	Дата и время восстановления оказания УПИ в случае приостановления их оказания	
10	Мероприятия по устранению неблагоприятных последствий инцидента с указанием планируемой и фактической продолжительности проведения данных мероприятий	
11 *	Дата восстановления оказания УПИ, соответствующего требованиям к оказанию услуг	
12	Неблагоприятные последствия инцидента по Субъектам Платежной системы, в том числе:	

12.1	- сумма денежных средств, уплаченных Оператором ПС и (или) взысканных с Оператора ПС	
12.2	- сумма денежных средств, уплаченных Оператором УПИ и (или) взысканных с Оператора УПИ	
12.3	- количество и сумма неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных Распоряжений Участников, на исполнение которых оказал влияние инцидент	
12.4 *	- продолжительность приостановления оказания УПИ	

Информация по п.п.1-5, 10, 12, 12.1, 12.2, 12.3 предоставляется всеми Субъектами ПС.

* Информация по п.п. 6, 9, 11, 12.4 дополнительно предоставляется Операторами УПИ.

**Информация по п.п. 7, 8 заполняется Оператором ПС.

Приложение №8 к Правилам Платежной системы МАРЛИН

МЕТОДИКА АНАЛИЗА И ОЦЕНКИ РИСКОВ В ПЛАТЕЖНОЙ СИСТЕМЕ МАРЛИН

1. Классификация рисков в Платежной системе МАРЛИН

1.1. Основными рисками, которые могут привести к нарушению БФПС, принимаются риски:

- операционный риск;
- расчетный риск (включающий в себя кредитный риск и риск ликвидности);
- правовой риск;
- общий коммерческий риск;
- системный риск.

1.2. **Операционный риск -** риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие возникновения у Субъектов Платежной системы сбоев, отказов и аварий в работе информационных и технологических систем, недостатков в организации и выполнении технологических и управленческих процессов, ошибок или противоправных действий персонала Субъектов Платежной системы, либо вследствие воздействия событий, причины возникновения которых не связаны с деятельностью Субъектов Платежной системы, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц.

Операционный риск обусловлен влиянием на Платежную систему операционных факторов в части неисправностей технологического обеспечения или возникшими операционными ошибками.

В состав операционного риска Платежной системы включаются риски информационной безопасности, возникающие вследствие недостатков процессов обеспечения защиты информации, в том числе недостатков применяемых технологических мер защиты информации, недостатков прикладного программного обеспечения автоматизированных систем и приложений, несоблюдения требований к указанным процессам деятельности операторами по переводу денежных средств, являющимися Участниками Системы, Операторами УПИ, а также ошибок или противоправных действий персонала Оператора и/или Субъектов Платежной системы.

В состав операционного риска Платежной системы включается риск взаимодействия с привлеченными поставщиками (провайдерами), предоставляющими услуги в сфере информационных технологий в целях оказания Оператором УПИ услуг платежной инфраструктуры, в том числе обусловленный вероятностью невыполнения поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг.

Общие принципы управления операционным риском состоят в применении Оператором, Операторами УПИ и Участниками следующих мер:

- регламентирование порядка выполнения основных процессов в Платежной системе в Правилах;
- регламентирование порядка совершения операций в рамках Правил Платежной системы МАРЛИН и 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 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;
- создание необходимых организационных и технических условий для обеспечения БФПС при совершении операций (на случай аварий, пожаров, терактов и других непредвиденных ситуаций);
- 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;
- обеспечение работоспособности аппаратно-программных комплексов всех Участников, 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 (далее - План ОНиВД);
  - проведение регулярной оценки качества и надежности функционирования информационных систем, операционных и технологических средств;
  - проведение регламентных работ.

1.3. **Расчетный риск** – риск Платежной системы, обусловленный влиянием на БФПС финансового состояния Участников, ЦПКК и Расчетного центра.

Расчетный риск включает:

- Кредитный риск – риск оказания УПИ, не соответствующего требованиям к оказанию услуг, ЦПКК или РЦ Платежной системы вследствие невыполнения Участниками Платежной системы договорных обязательств перед указанными организациями в установленный срок или в будущем;
- Риск ликвидности – риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие отсутствия у ЦПКК и (или) у Участников Платежной системы денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами Платежной системы.

Общие принципы управления расчетным риском состоят в контроле соблюдения Оператором Системы следующих процедур:

- выполнение Участниками требований по финансовому обеспечению расчетов в Платежной системе, контроль Оператором лимитов при авторизации Участников;
- выполнение ЦПКК требований по обеспечению достаточности денежных средств на Счетах ЦПКК для исполнения своих обязательств по переводу денежных средств;
- выполнение Оператором мониторинга объемов операций между Участниками, оперативный контроль резкого роста объемов операций того или иного Участника;
- возможность блокирования в случае угрозы возникновения риска Оператором Системы операций между Участниками.

Все операции по переводу денежных средств в Платежной системе осуществляются только при обязательном соблюдении следующих условий: сумма авторизационного запроса не превышает сумму доступного лимита, установленного ПКЦ и(или) РЦ на Участника.

1.4. **Правовой риск –** риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие несоблюдения Субъектами Платежной системы требований законодательства Российской Федерации, Правил Платежной системы, договоров, заключенных между Субъектами Платежной системы, документов Оператора Системы и документов Операторов УПИ либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации,

нормативных актах Банка России, Правилах Платежной системы и договорах, заключенных между Субъектами Платежной системы, а также вследствие нахождения Операторов УПИ и Участников под юрисдикцией различных государств.

Система управления правовым риском состоит в применении Оператором следующих способов минимизации данного вида риска:

- предварительная проверка Оператором потенциальных Участников и Операторов УПИ на обладание необходимой правоспособностью;
- мониторинг Оператором Системы информации об Участниках и Операторах УПИ в открытых источниках, либо периодическая, не реже одного раза в год, выборочная проверка Оператором Участников и Операторов УПИ на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров;
- организация оперативного процесса подготовки/внесения изменений, согласования и утверждения внутренних нормативных документов Оператора Системы в рамках меняющейся инфраструктуры Платежной системы, требований регулятора и/или вступлением в силу новых законопроектов;
- иные мероприятия.

1.5. **Общий коммерческий риск** – риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие ухудшения финансового состояния Оператора и/или Операторов УПИ, не связанного с реализацией кредитного риска Платежной системы и риска ликвидности Платежной системы.

Источниками и факторами общего коммерческого риска могут быть:

- использование устаревших технологий;
- негативная деловая репутация.

Общие принципы управления общим коммерческим риском состоят в применении Оператором, Операторами УПИ и Участниками следующих мер:

- использование прогрессивных технологий;
- поддержание позитивной деловой репутации;
- иные мероприятия.

1.6. **Системный риск** – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие неспособности одного или нескольких Субъектов Платежной системы исполнить принятые на себя обязательства или нарушений в самой Платежной системе, который вызовет неспособность большинства или всех Субъектов Платежной системы исполнить свои обязательства в срок. Таким образом, возникновение системного риска является следствием возникновения двух и более рисков, приведенных в пп. 1.2 - 1.5 настоящей Методики анализа рисков в Платежной системе МАРЛИН (далее – «Методика»).

1.7. Общие принципы управления системным риском зависят от причины его возникновения и состоят в применении мер, указанных в пп. 1.2 - 1.5 настоящей Методики.

2. Анализ бизнес-процессов в Платежной системе МАРЛИН

2.1. Оператор поддерживает перечни бизнес-процессов (Приложение №10 к Правилам) в актуальном состоянии. Для каждого бизнес-процесса определены риски, риск-события, причины их возникновения и возможные последствия.

2.2. Анализ бизнес-процессов, предусмотренных Приложением №10 к Правилам Платежной системы МАРЛИН, проводится Оператором путем:

- применения автоматизированных систем мониторинга работоспособности ПО Системы;
- фиксации выявленных нарушений в рамках определенных бизнес-процессов в базе (журнале) событий и инцидентов;

- расчета и анализа фактических значений показателей БФПС;
- сравнение фактических значений показателей БФПС с пороговыми уровнями, определенными Правилами;
- проведения оценки влияния выявленных инцидентов на БФПС.
- ведения перечня привлеченных Оператором поставщиков услуг, установления уровней оказания ими услуг и мониторинга качества их оказания;
- анализ полученной информации от Операторов УПИ о соблюдении уровня оказания услуг привлеченными ими поставщиками услуг (при привлечении);
- проведения анализа используемых Оператором и Операторами УПИ программных и технических средств, а также СКЗИ, применяемых для обеспечения функционирования Платежной системы, в том числе путем тестирования их работоспособности в условиях наступления непредвиденных и(или) чрезвычайных ситуаций;
- назначения ответственных сотрудников Оператора для осуществления контроля за соблюдением регламентов выполнения процедур.

2.3. При необходимости могут быть использованы иные способы анализа бизнес-процессов, не указанные в п. 2.2 настоящей Методики, позволяющие установить влияние различных факторов на БФПС.

2.4. В случае выявления в результате проводимого анализа процедур и(или) бизнес-процессов, не отраженных в Приложении №10 к Правилам, и(или) внедрения в Платежной системе МАРЛИН новых видов услуг и(или) продуктов, которые влекут за собой появление новых бизнес-процессов, не отраженных в Приложении №10 к Правилам, и которые могут оказать влияние на функционирование Платежной системы, Оператор проводит внеплановую оценку рисков в течение сроков, предусмотренных пп. 9.8.1.1 Правил, в рамках которой формирует новый перечень бизнес-процессов, формирует перечни рисков и риск-событий для каждого бизнес-процесса с указанием причин риск-событий и их последствий, вносит изменения в классификаторы рисков. По итогам внеплановой оценки рисков Оператор актуализиует профили риска.

3. Порядок выявления и анализа рисков Платежной системы, включая выявление риск-событий, и порядок определения для каждого из выявленных риск-событий уровня риска

3.1. Анализ и оценка рисков в Платежной системе МАРЛИН осуществляется Оператором с применением методов, соответствующих Стандарту:
- Метод номинальной группы;
- Сценарный анализ с использованием статистических данных, 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;
- Матрица вероятности и последствий.

*3.2. **Выявление риск-событий***

3.2.1. По каждому из видов рисков в ПС, указанных в пп. 1.2 – 1.5. настоящей Методики могут произойти следующие риск-события:

а) по операционному риску:

- нарушение работоспособности аппаратно-программных комплексов Оператора и/или Субъектов Платежной системы;
- нарушение сроков выполнения временного регламента Оператором и/или Субъектами Платежной системы;
- воздействие событий, причины возникновения которых не связаны с деятельностью Оператора и/или Субъектов Платежной системы;
- нарушение порядка обеспечения защиты информации.

б) по расчетному риску:

- невыполнение Участниками договорных обязательств перед РЦ и (или) ЦПКК в установленный срок или в будущем (кредитный риск);
- отсутствие у ЦПКК и (или) у Участников денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами Платежной системы (риск ликвидности).

в) по правовому риску:

- претензии правового характера к Субъектам Платежной системы со стороны государственных органов власти, ЦБ РФ
- претензии правового характера к Субъектам Платежной системы со стороны других Субъектов Платежной системы, Клиентов Участников.
- нахождение Оператора, Операторов УПИ и Участников под юрисдикцией различных государств.

г) по общему коммерческому риску:

- ухудшение финансового состояния Оператора и (или) Операторов УПИ, не связанного с реализацией кредитного риска и риска ликвидности Платежной системы.

д) по системному риску:

- распространение между Субъектами Платежной системы последствий сочетания двух основных рисков, указанных в пп. 1.2–1.5 настоящей Методики, вызывающих нарушения функционирования Платежной системы;
- распространение между Субъектами Платежной системы последствий сочетания нескольких (более двух) основных рисков, указанных в пп. 1.2–1.5 настоящей Методики, вызывающих нарушения функционирования Платежной системы.

3.2.2. Перечень риск-событий может корректироваться с учетом изменений и дополнений.

3.3. ***Порядок определения уровня риска***

3.3.1. Уровень риска рассчитывается по каждому риск-событию на основании комплексной оценки риска, определяемой вероятностью наступления риск-событий в зависимости от причины их возникновения и величиной возможных последствий их реализации с использованием формулы:

R=I*P (1)

где:

R - уровень риска

I - последствие риск-события

P - вероятность наступления риск-события.

3.3.2. Для оценки вероятности наступления риск-событий и последствий их реализации используются методы количественной оценки рисков.

3.3.3. Количественная оценка вероятности наступления риск-события

3.3.3.1. Для каждого вида рисков определен метод количественной оценки вероятности наступления риск-события, обусловленный следующими факторами:

а) Операционный риск. Оценка вероятности наступления операционного риска обусловлена многообразием факторов и источников данного вида риска:

- *внутренние источники (вследствие возникновения у Субъектов Платежной системы):*
  - сбоев, отказов и аварий в работе информационных и технологических систем, оборудования;
  - недостатков в организации и выполнении технологических и управленческих процессов (в том числе, несовершенство организационной структуры в части распределения полномочий подразделений и сотрудников, порядков и процедур совершения операций в рамках Платежной системы, их документирования и отражения в учете);

- ошибок или противоправных действий персонала Субъектов Платежной системы (несоблюдение сотрудниками установленных порядков и процедур, внутренних регламентов взаимодействия вследствие непреднамеренных или умышленных действий);

- *внешние источники (вследствие воздействия событий, причины возникновения которых не связаны с деятельностью Субъектов Платежной системы):*
  - чрезвычайные ситуации;
  - ошибочные действия третьих лиц (физических и юридических);
  - противоправные действия третьих лиц (физических и юридических);
- *риски информационной безопасности*:
  - риск преднамеренных действий со стороны работников Субъектов Платежной системы и (или) третьих лиц с использованием программных и (или) программно-аппаратных средств, направленных на объекты информационной инфраструктуры Субъектов Платежной системы в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности информации, подготавливаемой, обрабатываемой и хранимой такими объектами, а также в целях несанкционированного присвоения, хищения, изменения, удаления данных и иной информации (структуры данных, параметров и характеристик систем, программного кода) и нарушения режима доступа;
  - Инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
  - другие виды риска информационной безопасности, связанных с обработкой (хранением, уничтожением) информации без использования объектов информационной инфраструктуры.

б) Расчетный риск. Оценка вероятности наступления расчетного риска обусловлена тем, что Участники и ЦПКК обязаны обеспечить наличие денежных средств на Счетах, открытых в РЦ, до завершения расчетов.

в) Правовой риск. Оценка вероятности наступления правого риска обусловлена определением количества выявленных фактов в заданный временной интервал претензий правового характера к Субъектам Платежной системы со стороны:

- государственных органов власти;
- Центрального Банка Российской Федерации;
- других Субъектов Платежной системы;
- Клиентов Участников.

г) Общий коммерческий риск. Для количественной оценки вероятности наступления общего коммерческого риска проводится статистический анализ ухудшения финансового состояния Оператора и/или Операторов УПИ, не связанного с реализацией кредитного риска и риска ликвидности.

д) Системный риск. Для количественной оценки вероятности наступления системного риска проводится статистический анализ неспособности одного или нескольких Субъектов Платежной системы исполнить принятые на себя обязательства или нарушений в самой ПС, которые могут повлечь за собой неспособность большинства или всех Субъектов Платежной системы исполнить свои обязательства в срок.

3.3.3.2. На основе статистической обработки информации Оператор выявляет периодичность возникновения внутренних и внешних факторов риска и дает оценку вероятности риск-события согласно указанной методике.

3.3.3.3. Оценка вероятности наступления риск-события в зависимости от причины возникновения производится по пятибалльной шкале:

- Практически невозможно (от 0 до 2 раз в квартал);
- Маловероятно (от 2 до 5 раз в квартал);
- Возможно (от 5 до 10 раз в квартал)
- Вполне вероятно (от 10 до 15 раз в квартал)
- Высокая вероятность (более 15 раз в квартал)

3.3.4. *Количественная оценка последствия реализации риск-событий*:

3.3.4.1. Для количественной оценки последствия риск-событий проводится количественная оценка размера причиняемого ущерба от реализации нарушения БФПС:

- потери Оператора от невозможности проведения операций;
- потери Операторов УПИ от невозможности проведения операций;
- потери Участников от невозможности проведения операций;
- штрафы, которые должны будут выплатить Оператор, Операторы УПИ и Участники ввиду нарушения законодательства.

3.3.4.2. Количественная оценка рассчитывается на основе среднего количества операций за единицу времени простоя и потерь Субъектов Платежной системы и Клиентов от невозможности проведения одной операции.

3.3.4.3. Время простоя определяется для каждого риск-события отдельно и напрямую влияет на результаты количественной оценки.

3.3.4.4. Оценка последствия риск-события производится по пятибалльной шкале и отражает возможность функционирования ПС и финансовые потери в случае наступления риска:

- *Минимальное воздействие*: наступление риска не приведет к временной неработоспособности отдельных сервисов (не влияет на возможность ведения основной деятельности), позволяет системе оказывать УПИ в стандартном режиме и приводит к несущественным затратам (менее 100 тыс. рублей в год) на устранение фактора риска.
- *Умеренное воздействие*: наступление риска может привести к временной неработоспособности отдельных сервисов, УПИ оказываются в стандартном или разрешенном режиме, может приводить к допустимым затратам (от 100 до 300 тыс. рублей в год) на устранение фактора риска.
- *Существенное воздействие*: наступление риска может привести к неработоспособности отдельных сервисов (влияет на возможность ведения основной деятельности), приводит к существенным затратам (от 300 до 500 тыс. рублей в год) на устранение фактора риска.
- *Значительное воздействие*: наступление риска может привести к неработоспособности отдельных сервисов (влияет на возможность ведения основной деятельности), приводит к значительным затратам (от 500 тыс. до 1 млн. рублей в год) на устранение фактора риска.
- *Катастрофическое воздействие*: наступление риска оказывает влияние на возможность бесперебойного функционирования платежной системы (оказание УПИ в критическом режиме) и приводит к катастрофическим затратам (свыше 1 млн. рублей в год) на устранение фактора риска.

3.3.5. Комплексная модель оценки уровня риска строится следующим образом:

				Величина возможных последствий реализации Риск-события				
				Минимальное воздействие	**Умеренное воздействие**	**Существенное воздействие**	**Значительное воздействие**	**Катастрофическое воздействие**
				баллы				
				1	2	3	4	5
Вероятность наступления Риск-события	**высокая вероятность**	**баллы**	5	**5**	**10**	**15**	**20**	**25**
	вполне вероятно		4	**4**	**8**	**12**	**16**	**20**
	возможно		3	**3**	**6**	**9**	**12**	**15**
	маловероятно		2	**2**	**4**	**6**	**8**	**10**
	практически невозможно		1	**1**	**2**	**3**	**4**	**5**

3.3.6. В результате использования комплексной модели уровня риска выделяются следующие уровни рисков:

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***

Уровень риска (u)	0 (1 - 4 баллов)	1 (5 - 9 баллов)	2 (10 - 12 баллов)	3 (свыше 12 баллов)

4. Порядок определения для каждого из выявленных рисков в Платежной системе уровня присущего риска, а также уровня допустимого риска

4.1. Уровень присущего риска определяется по каждому риск-событию путем сложения величин, рассчитанных по формуле (1) по каждой причине возникновения риск-события.

4.2. В Платежной системе устанавливается уровень допустимого риска не выше 2 - **средний**. Уровень допустимого Системного риска в Платежной системе определен в п. 7.3.1 Методики.

4.3. В целях поддержания допустимого уровня рисков нарушения БФПС определен перечень способов управления рисками для каждого риск-события, указанных в профиле рисков, а также определены процедуры, мероприятия и способы достижения и поддержания допустимого уровня рисков.

5. Порядок определения рисков, значимых для Платежной системы

5.1. Уровень присущего риска по каждому риск-событию сравнивается с уровнем допустимого риска.

5.2. В случае, если уровень присущего риска до применения способов управления рисками в платежной системе может превысить или превысил уровень допустимого риска, данный риск считается значимым для Платежной системы.

5.3. Оператор выделяет риски, значимые для Платежной системы, и применяет способы управления для каждого из таких рисков.

6. Порядок определения уровня остаточного риска. Мониторинг рисков

6.1. Уровень остаточного риска определяется аналогично порядку определения уровня присущего риска по формуле:

RR=II*PP (2)

где:

RR - уровень остаточного риска

II - последствие риск-события с учетом внедрённых способов управления рисками

PP - вероятность наступления риск-события с учетом внедренных способов управления рисками.

6.2. Результаты оценки уровня остаточного риска фиксируются для каждого риск-события, указанного в профилях рисков Платежной системы. Профили рисков должны поддерживаться в актуальном состоянии и регулярно обновляться.

6.3. В случае превышения уровня остаточного риска над уровнем допустимого риска по любому из значимых рисков в Платежной системе МАРЛИН, Оператор инициирует процедуру принятия решения о необходимости применения дополнительных способов управления рисками, которая включает следующие мероприятия:

- выявление причин неэффективности ранее примененных способов управления риском;
- формирование перечня дополнительных способов управления рисками;
- анализ влияния дополнительных мер на эффективность функционирования Платежной системы.

6.4. Решение о необходимости применения дополнительных способов управления рисками принимается единоличным исполнительным органом Оператора на основании информации от сотрудника (структурного подразделения) Оператора, ответственного за управление рисками.

6.5. Решение единоличного исполнительного органа Оператора оформляется приказом и может влечь за собой:

- пересмотр установленных в Системе лимитов и иных требований к работе в Системе, включая пересмотр причин (источников) возникновения риск-события, вероятность их наступления, способов мониторинга рисков и методов реагирования и т.д.;
- модернизацию программно-технических средств Системы;
- внесение изменений в настоящие Правила и (или) внутренние документы Оператора.

6.6. После реализации дополнительных способов управления рисками Оператор проводит внеплановую оценку уровня остаточного риска для подтверждения его соответствия допустимому уровню.

6.7. Мониторинг рисков в Платежной системе, в том числе уровня остаточного риска после применения способов управления рисками в платежной системе, его соответствия уровню допустимого риска, осуществляются по каждому виду рисков, предусмотренных профилями рисков, на регулярной основе с учетом требований Правил, внутренних документов Оператора и действующего законодательства.

6.8. К перечню мероприятий, выполняемых в рамках мониторинга рисков в Платежной системе, относятся, в том числе:

6.8.1. применение автоматизированных систем мониторинга работоспособности ПО Системы для оперативного выявления происходящих в Системе риск-событий, в том числе которые привели к инциденту;
6.8.2. регулярный анализ произошедших в Системе риск-событий (включая поступление претензий);
6.8.3. контроль установленного доступного лимита Участнику в ПО Системы, в пределах которого разрешается проведение операций в Системе, изменяющегося при авторизации каждой операции перевода денежных средств;
6.8.4. контроль своевременности проведения расчетов в Системе;
6.8.5. проведение оценки влияния выявленного инцидента на БФПС;
6.8.6. сравнение фактических значений показателей БФПС с установленными Правилами пороговыми уровнями показателей БФПС;
6.8.7. сравнение фактического уровня реализовавшегося риска с установленным уровнем допустимого риска;
6.8.8. применение ответственными сотрудниками Оператора мер реагирования (в том числе дополнительных) при нарушении порогового уровня показателей БФПС;
6.8.9. поддержание актуального перечня риск-событий по каждому виду рисков в разрезе бизнес-процессов;
6.8.10. своевременная актуализация профилей рисков, в том числе профиля риска нарушения БФПС, как механизм непрерывного мониторинга и оценки соответствия уровня остаточного риска;
6.8.11. иные мероприятия, позволяющие обеспечить оперативное выявление рисков в Платежной системе, включая контроль соблюдения Субъектами Правил Платежной системы МАРЛИН, соответствие критериям, установленным для соответствующего Субъекта и др.

7. Перечень риск-событий, причин риск-событий и способов управления рисками Платежной системы.

7.1. Перечень риск-событий, причин риск-событий и способов управления рисками Платежной системы с указанием на уровень присущего риска, уровень допустимого риска, а также уровень остаточного риска) в разрезе операционного, расчетного, правового, общего коммерческого и системного рисков содержится в соответствующих профилях риска в Приложении №11 к Правилам.

7.2. Профиль риска нарушения БФПС составляется по всем значимым рискам Платежной системы и содержится в Приложении №12 к Правилам.

7.3. Порядок определения уровня **Системного риска**

7.3.1. Уровень Системного риска рассчитывается как сумма уровней двух или более рисков, значимых для Платежной системы:

Категория риска	**без риска**	**низкий**	**средний**	**высокий**
Уровень Операционного риска	0	1	2	3
Уровень Расчетного риска	0	1	2	3
Уровень Правового риска	0	1	2	3
Уровень Общего коммерческого риска	0	1	2	3
Уровень Системного риска	**0**	**4**	**8**	**12**

Уровень допустимого Системного риска в Платежной системе устанавливается не более 8 включительно.

Приложение №9 к Правилам Платежной системы МАРЛИН

Методика оценки рисков нарушения БФПС в Платежной системе МАРЛИН

1. При оценке рисков нарушения БФПС Оператор, в соответствии со Стандартом, использует методы, соответствующие Стандарту:

   – Индекс риска;
   – Анализ влияния на бизнес (BIA).

2. В соответствии с Методикой анализа и оценки рисков в Платежной системе (Приложение №8 к Правилам) устанавливаются следующие уровни рисков:

Категория риска	**Без риска**	**Низкий**	**Средний**	**Высокий**
Уровень риска (u)	0	1	2	3

3. В Платежной системе установлен допустимый уровень рисков нарушения БФПС в соответствии с Методикой анализа и оценки рисков в Платежной системе, включая профили рисков в соответствии с требованиями нормативных актов Банка России (Приложение №8 к Правилам):

Категория риска	**Допустимый уровень рисков нарушения БФПС**
Операционный риск	<=2
Расчетный риск	<=2
Правовой риск	<=2
Общий коммерческий риск	<=2
Системный риск	<=8

4. Допустимые уровни рисков нарушения БФПС могут быть изменены путем внесения изменений в настоящее Приложение или по результатам оценки рисков в Платежной системе.
5. В процессе функционирования Платежной системы Оператор может выявить иные факторы рисков и установить дополнительные показатели БФПС.
6. Оценка уровня риска нарушения БФПС рассчитывается на основе оценок основных рисков.

6.1. Для оценки применяется критерий 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.). Критерий доступности рассчитывается по следующей формуле:

$$d = (1 — t / T)$$

где ***d*** – критерий 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 этом значение ***d = 1*** соответствует функционированию без сбоев в течение заданного временного интервала. Значение ***d* = 0** возможно в случае неработоспособности в течение заданного временного интервала.

6.2. Уровень риска нарушения БФПС устанавливается в соответствии с конкретными значениями показателей доступности, попадающими в заданные интервалы.

6.3. Процедуру анализа рисков нарушения БФПС осуществляют внутренние структурные подразделения Оператора, 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.

6.4. Принятие мер, необходимых для достижения или поддержания допустимого уровня каждого из видов рисков нарушения БФПС, осуществляется внутренним структурным подразделением Оператора, ответственным за анализ и контроль соответствующего риска. Управление рисками осуществляют уполномоченные органы и подразделения Оператора в соответствии со своими полномочиями.

6.5. Выявление текущих изменений присущего уровня риска нарушения БФПС осуществляется ответственными структурными подразделениями Оператора на регулярной основе в сроки, предусмотренные регламентирующими процесс управления рисками внутренними нормативными документами.

6.6. В целях управления рисками нарушения БФПС Оператор осуществляет информационное взаимодействие с Субъектами Платежной системы в соответствии с порядком информационного взаимодействия Субъектов Платежной системы и документационного обеспечения их деятельности по обеспечению БФПС.

7. Порядок оценки операционного риска.

Источником операционного риска (ОР) является нарушение работоспособности аппаратно-программных комплексов (снижение производительности и/или выход из нормального режима функционирования отдельной подсистемы или сервиса, или всех сервисов Платежной системы, включая невозможность проведения ни одной операции у одного или нескольких Участников, в том числе вследствие нарушений требований к обеспечению защиты информации при осуществлении переводов денежных средств), ненадлежащие действия персонала, а также неэффективная деятельность внутренних структурных подразделений (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), а также невыполнение поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг.

7.1. Локализацией (местом проявления) ОР являются структурные подразделения и аппаратно-программные комплексы Субъектов Платежной системы, в разрезе которых осуществляется контроль проявления операционного риска.

7.2. Формой реализации ОР являются нарушения функционирования Платежной системы в результате нарушения работоспособности аппаратно-программных комплексов Субъектов Платежной системы, выполнения недопустимых операций или ошибочного выполнения операций в Платежной системе, нарушения порядка обеспечения защиты информации, невыполнения поставщиками услуг (провайдерами) своих обязательств.

7.3. Оценка ОР применяется к оценке оказания услуг в случаях:

- нарушения работоспособности аппаратно-программных комплексов и ненадлежащих действий персонала;
- невыполнения поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг;

– нарушения порядка обеспечения защиты информации.

7.3.1. В случае реализации события, затрагивающего все подсистемы и/или сервисы Платежной системы, при невозможности проведения ни одной операции, повлекшего за собой недоступность услуг платежной инфраструктуры с учетом того, что ОР может проявляться круглосуточно, Т = 1440 мин.

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***
Пороговые значения t (мин)	0	10	30	60
Интервалы t[1] (мин.)	t<=10	10<t<=30	30<t<=60	t>60
Пороговые значения ОР	ОР>=0,993	0,979<=ОР<0,993	0,958<=ОР<0,979	ОР<0,958
Уровень риска (УОР)	0	1	2	3

7.3.2. Критерий доступности может применяться к оценке оказания услуг (с учетом иных временных интервалов t и Т, соответствующих временному регламенту их функционирования).

7.4. Система управления ОР предусматривает следующие способы и мероприятия по управлению риском:

7.4.1. 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:
- контроль качества предоставляемой услуги (выполняемой работы).

7.4.2. По персоналу:

- ограничение функций и полномочий сотрудников;
- обучение персонала новым информационным технологиям, повышение его квалификации, периодическое тестирование.

8. Порядок оценки расчетного риска (кредитного риска и риска ликвидности).

8.1. Источником расчетного риска (РР) является недостаточность (отсутствие) средств у Участника или нескольких Участников, и (или) у ЦПКК для своевременного выполнения ими своих расчетных обязательств перед другими Участниками (в том числе являющимися участником или расчетным центром платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие) и Оператором, финансовая несостоятельность Участника и (или) ЦПКК, концентрация значительного объема расчетных документов в определенные моменты и (или) периоды времени в течение дня, вероятность возникновения которых обусловлена особенностями Платежной системы 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

[1] Время, выраженное в секундах, округляется до целого значения минут путем отбрасывания значений секунд

депонировании денежных средств, выполнение процедур неттинга, процедуры управления очередью расчетных документов).

8.2. Локализацией (местом проявления) РР являются Счета Участников и ЦПКК, показатели состояния этих Счетов, контроль за которыми позволяет выявить предпосылки реализации риска (например, количество и величина «чистых» дебетовых позиций отдельных Участников, наличие, состав и величина очередей неисполненных расчетных документов).

8.3. Формой реализации РР являются нежелательные изменения показателей, характеризующих несвоевременность проведения Участником или ЦПКК расчетов (например, время задержки исполнения расчетных документов, отсутствие денежных средств на Счетах Участников и (или) ЦПКК или невозможность использования имеющихся на этих Счетах остатков денежных средств, невозможность исполнения Участником и (или) ЦПКК своих обязательств в Платежной системе).

8.4. Оценка РР осуществляется следующим образом:

8.4.1. Оценка РР осуществляется с учетом того, что t — число операционных дней нарушения оказания расчетных услуг, Т — среднее число операционных дней в течение месяца, Т = 21 день.

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***
Пороговые значения t (дни)	0	5	10	15
Интервалы t (дни)	t<=5	5<t<=10	10<t<=15	t>15
Пороговые значения РР	РР>=0,762	0,524<=РР<0,762	0,286<=РР<0,524	РР<0,286
Уровень риска (УРР)	0	1	2	3

Для одновременной оценки уровня РР при урегулировании всеми Участниками «чистых» дебетовых позиций в пределах клирингового цикла и по итогам осуществления расчетов с ЦПКК в приведенном выше расчете вместо t применяется tcp. — среднее число операционных дней нарушения расчетных услуг в течение месяца, Т — среднее число операционных дней в течение месяца, Т = 21 день. Величина tcp рассчитывается по следующей формуле (2):

$$t_{ср.} = (t_1 + t_2 + \ldots + t_n) / n, \quad (2)$$

где

t_i - число операционных дней в течение месяца, когда по i-му Участнику Платежной системы и ЦПКК нарушены расчетные услуги (i=1, 2, … , n),

n - число Участников Платежной системы и ЦПКК.

8.5. Система управления РР предусматривает следующие способы и мероприятия по управлению рисками:

8.5.1. Установление предельных размеров (лимитов) обязательств Участникам с учетом уровня риска.

8.5.2. Финансовый анализ и мониторинг деятельности Участника.

9. Порядок оценки Правового риска.

9.1. Источником правового риска (ПР) является несоблюдение Субъектами Платежной системы требований законодательства, нормативных актов и заключенных договоров, внутренних документов, регламентирующих их деятельность, а также наличие недостатков внутренних документов.

9.2. Локализацией (местом проявления) ПР являются:

- Субъекты Платежной системы, которым могут быть предъявлены претензии правового характера, связанные с несоблюдением требований законодательства, нормативных актов и заключенных договоров;

- внутренние документы Субъектов Платежной системы и договоры, содержание которых подлежит постоянному контролю на соответствие законодательству и нормативным актам, с учетом вносимых в них изменений.

9.3. Формой реализации ПР являются претензии правового характера к Субъектам Платежной системы со стороны других Субъектов Платежной системы, со стороны государственных органов, со стороны Клиентов Участников.

9.3.1. Оценка ПР рассчитывается с учетом того, что t — число претензий к Субъектам Платежной системы 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
Интервалы t (раз)	t<=2	2<t<=3	3<t<=4	t>4
Пороговые значения ПР	ПР>=0,995	0,992<=ПР<0,995	0,989<=ПР<0,992	ПР < 0,989
Уровень риска (УПР)	0	1	2	3

Для одновременной оценки ПР при урегулировании всеми Субъектами Платежной системы ПР в приведенном выше расчете вместо t применяется tcp. — сумма среднего числа претензий к каждой группе Субъектов Платежной системы в течение года, t —дней в году, T = 365 день. Величина tcp рассчитывается по следующей формуле:

$$t_{cp.} = (t_1 + t_2 + \ldots + t_n) / n_1 + (t_1 + t_2 + \ldots + t_n) / n_2 + (t_1 + t_2 + \ldots + t_n) / n_3$$

где

t_i - число претензий к каждой группе Субъектов Платежной системы, когда i-му Субъекту Платежной системы получена претензия (i=1, 2, … , n),

n — число Субъектов[1] Платежной системы в группе[2].

9.4. Система управления ПР предусматривает следующие мероприятия по управлению риском:

9.4.1. предварительная проверка Оператором потенциальных Участников и Операторов УПИ на обладание необходимой правоспособностью (в соответствии с Правилами Платежной системы МАРЛИН);

9.4.2. периодическая, не реже одного раза в два года, выборочная проверка Оператором Участников и/или Операторов УПИ на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров.;

9.4.3. организация оперативного процесса подготовки/внесения изменений, согласования и утверждения внутренних нормативных документов Оператора в рамках меняющейся инфраструктуры Платежной системы, требований регулятора и/или вступлением в силу новых законопроектов;

9.4.4. иные мероприятия.

10. Порядок оценки общего коммерческого риска.

---

1 В случае, когда Субъект одновременно выполняет две и более функций, Субъект считается единожды в любой из групп Субъектов (например, Банк одновременно и Участник и РЦ)

2 Группа Субъектов: 1 группа - Субъекты, оказывающие Операционные услуги, услуги платежного клиринга; 2 группа - Субъекты, оказывающие Расчетные услуги; 3 группа – Субъекты, являющиеся Участниками

10.1. Источником общего коммерческого риска (ОКР) является наличие негативной информации о Субъектах Платежной системы и использование неконкурентноспособного оборудования.

10.2. Локализацией (местом проявления) ОКР являются:

- наличие негативной информации о Субъектах Платежной системы в информационно-телекоммуникационной сети «Интернет», других СМИ;
- технологическое отставание Субъектов Платежной системы.

10.3. Формой реализации ОКР являются сокращение количества Клиентов, сокращение количества Участников.

10.3.1. Оценка ОКР осуществляется с учетом того, что t — число негативных публикаций о Субъектах Платежной системы в течение года, Т = 365 дней.

Категория риска	***Без риска***	***Низкий***	***Средний***	***Высокий***
Пороговые значения t (раз)	0	1	2	3
Интервалы t (раз)	t<=1	1<t<=2	2<t<=3	t>3
Интервалы ОКР	ОКР>=0,997	0,995<=ОКР<0,997	0,992<=ОКР<0,995	ОКР<0,992
Уровень риска (УОКР)	0	1	2	3

Для одновременной оценки ОКР всех или нескольких Субъектов Платежной системы в приведенном выше расчете вместо t применяется tcp. — сумма среднего числа негативных публикаций о Субъектах Платежной системы в течение года, Т —дней в году, Т = 365 день. Величина tcp рассчитывается по следующей формуле:

$$t_{ср.} = (t_1 + t_2 + \ldots + t_n) / n_1 + (t_1 + t_2 + \ldots + t_n) / n_2 + (t_1 + t_2 + \ldots + t_n) / n_3,$$

где

t_i - число негативных публикаций к каждой группе Субъектов Платежной системы, когда по i-му Субъекту Платежной системы обнаружена негативная публикация (i=1, 2, … , n),

n — число Субъектов[1] Платежной системы в группе[2].

10.4. Система управления ОКР предусматривает следующие мероприятия по управлению риском:

10.4.1. Поддержание положительной деловой репутации Субъектов Платежной системы, выполнение требований законодательных, нормативных документов, Правил, договоров, публикации в СМИ руководителей Субъектов Платежной системы.

10.4.2. Использование современного технологического обеспечения и технических средств.

10.4.3. Иные мероприятия.

11. Порядок оценки Системного риска.

11.1. Источником системного риска (СР) является реализация одновременно нескольких или всех рисков, указанных в п. 7 – п. 10 настоящего Приложения. СР возникает вследствие неспособности одного или нескольких Субъектов Платежной системы исполнить принятые на себя обязательства или нарушений в самой Платежной системе, которая вызовет неспособность большинства или всех Субъектов Платежной системы исполнить свои обязательства в срок.

11.2. Локализацией (местом проявления) СР являются элементы Платежной системы, контроль за которыми позволяет выявить предпосылки реализации СР (например, количество и величина наиболее крупных «чистых» дебетовых позиций Участников, наличие, состав и величина очередей

[1] В случае, когда Субъект одновременно выполняет две и более функций, Субъект считается единожды в любой из групп Субъектов (например, Банк одновременно и Участник и РЦ)

[2] Группа Субъектов: 1 группа - Субъекты, оказывающие Операционные услуги, услуги платежного клиринга; 2 группа - Субъекты, оказывающие Расчетные услуги; 3 группа – Субъекты, являющиеся Участниками

неисполненных распоряжений, работоспособность основных аппаратно-программных комплексов и др.).

11.3. Формой реализации СР является распространение между Субъектами Платежной системы последствий основных рисков, указанных в п. 7 – п. 10 настоящего Приложения, вызывающих нарушения функционирования Платежной системы.

11.4. Уровень СР рассчитывается как сумма уровней основных рисков, указанных в п. 7 – п. 10 настоящего Приложения.

11.5. Система управления рисками в целях предотвращения и минимизации СР предусматривает предотвращение и минимизацию основных рисков, указанных в п. 7 – п. 10 настоящего Приложения.

Приложение №10 к Правилам Платежной системы МАРЛИН

Бизнес-процессы Платежной системы МАРЛИН

Бизнес-процессы	Процедуры	Код
Операционные услуги	**Проверка возможности осуществления операций:** Прием и обработка распоряжений Участников Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников	1.1.
	Передача обработанных распоряжений Участников в ПКЦ	1.2.
Услуги платежного клиринга	Прием распоряжений, поступивших из ОЦ	2.1.
	Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений): - удостоверение права распоряжения денежными средствами (удостоверение права использования электронного средства платежа); - контроль целостности распоряжений; - структурный контроль распоряжений; - контроль значений реквизитов распоряжений; - контроль достаточности денежных средств	2.2.
	Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению	2.3.
	Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ	2.4.
Расчетные услуги	Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК	3.1.
	Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК	3.2.

Приложение №11 к Правилам Платежной системы МАРЛИН

ПРОФИЛИ РИСКОВ ПЛАТЕЖНОЙ СИСТЕМЫ МАРЛИН

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, *(Р) (в баллах, согласно п. 3.3..5 Приложения №8 к Правилам)*	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события, *(I) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которые влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска (R) *(согласно пп. 3.3.1, 4.1 Приложения №8 к Правилам,* R = Σ Pi*Ii, *при i=1…n, n - кол-во источников риск-события)*	Уровень допустимого риска *(в соответствии с п. 4.2 Приложения №8 к Правилам)*	Применяемые способы управления рисками	Уровень остаточного риска, (RR) *(рассчитывается аналогично уровню присущего риска после применения способов управления рисками согласно п. 6.1 Приложения №8 к Правилам)*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1.1.	**Операционный**	Нарушение работоспособности аппаратно-программных комплексов Оператора ПС и/или Субъектов ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	возникновение сбоев, отказов и аварий в работе информационных и технологических систем, оборудования	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК, Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и/или ЦПКК	4	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность или задержка каждого Бизнес-процесса некорректное исполнение Бизнес-процесса 1.1. нарушение договорных обязательств влияние на значения показателей БФПС.	3	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	24 балла, что соответствует Уровню риска 3	2	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; 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.	1
				нарушения в каналах связи, электричества			2			1							
				недостатки в организации и выполнении технологических и управленческих процессов			1			2							
				использование устаревших программно-аппаратных средств и технологий			1			2							

				ошибки или противоправные действия персонала Оператора ПС и/или Субъектов ПС	и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)		2			3		и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)					
1.2.	**Операционный**	Нарушение сроков выполнения Временного регламента Оператором ПС и/или Субъектами ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	возникновение сбоев, отказов и аварий в работе информационных и технологических систем, оборудования нарушения в каналах связи, электричества недостатки в организации и выполнении технологических и управленческих процессов ошибки или противоправные действия персонала Оператора ПС и/или Субъектов ПС	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК, Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и)	3 2 1 1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность осуществления или задержка каждого Бизнес-процесса нарушение договорных обязательств влияние на значения показателей БФПС.	3 1 2 1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	14 баллов, что соответствует Уровню риска 3	2	регламентирование порядка выполнения основных процессов в ПС в Правилах; регламентирование порядка совершения операций в рамках Правил и 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; разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев; 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.	1
1.3.	Операционный	Воздействие событий, причины возникновения которых не связаны с деятельностью Оператора ПС и/или Субъектов ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятност	чрезвычайные ситуации	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и)	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функциони	невозможность осуществления или задержка каждого Бизнес-процесса нарушение договорных обязательств	3	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	24 балла, что соответствует Уровню риска 3	2	создание необходимых организационных и технических условий для обеспечения БФПС при совершении операций (на случай аварий, пожаров, терактов и других непредвиденных ситуаций); разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев; поиск новых направлений развития	1

			и и последствий.	обстоятельства непреодолимой силы, в том числе политические внешнеэкономические факторы	ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	и/или ЦПКК	3	рования системы	влияние на значения показателей БФПС.	5		ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)					
				ошибочные действия третьих лиц (физических и юридических)			1			3							
				противоправные действия третьих лиц (физических и юридических).			1			3							
1.4.	Операционный	Нарушение порядка обеспечения защиты информации	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	ошибки или противоправные действия персонала Оператора ПС и/или Субъектов ПС	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и/или ЦПКК	3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность или задержка каждого Бизнес-процесса нарушение договорных обязательств влияние на значения показателей БФПС.	4	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	27 баллов, что соответствует Уровню риска 3	2	обеспечение информационной безопасности; контроль над доступом к информации; применение многоуровневой защиты информации с использованием сертифицированных средств защиты информации; регламентирование процессов защиты информации; применение принципов разделения и ограничения функций в целях определения предела полномочий сотрудников, осуществляющих операции.	1
				недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации			1			3							
				недостатки прикладного программного обеспечения автоматизированных систем и приложений			3			3							

				несоблюдение требований к указанным процессам деятельности операторами по переводу денежных средств, являющимися Участниками Системы, Операторами УПИ	и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)		1			3		и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)					
1.5.	Операционный	Нарушение работоспособности систем и сервисов, предоставляемых привлеченными поставщиками и (провайдерами)	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	ошибки или противоправные действия персонала Оператора ПС и/или Субъектов ПС	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и/или ЦПКК	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность или задержка каждого Бизнес-процесса нарушение договорных обязательств влияние на значения показателей БФПС	2	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	15 баллов, что соответствует Уровню риска 3	2	проверка поставщика (провайдера) перед заключением договора анализ проекта договора на предмет наличия и содержания условий об уровне качества предоставляемых услуг (SLA) контроль качества предоставляемой услуги (выполняемых работ) 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 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	1
				нарушение договорных обязательств Оператором или поставщиком (провайдером)			2			2							
				нарушения функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, предоставляемого привлеченными поставщиками (провайдерами)			3			3							

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, *(P) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события, *(I) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которые влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска (R) *(согласно пп. 3.3.1, 4.1 Приложения №8 к Правилам, R = Σ Pi*Ii, при i=1…n, n - кол-во источников риск-события)*	Уровень допустимого риска *(в соответствии с п. 4.2 Приложения №8 к Правилам)*	Применяемые способы управления рисками	Уровень остаточного риска, (RR) *(рассчитывается аналогично уровню присущего риска после применения способов управления рисками согласно п. 6.1 Приложения №8 к Правилам)*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1.1.	**Расчетный**	Невыполнение Участниками договорных обязательств перед РЦ и (или) ЦПКК в установленный срок или в будущем (кредитный риск)	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	недостаточность (отсутствие) средств у Участника или у нескольких Участников, для своевременного выполнения ими своих расчетных обязательств РЦ и (или) ЦПКК платежной системы, с которым Оператор Системы осуществляет межсистемное взаимодействие	Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.)	ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	1	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения процедуры приема к исполнению распоряжений Участников невозможность исполнения распоряжений ПКЦ и (или) ЦПКК о проведении расчетов с Участниками; возникновение дебиторской задолженности; нарушение договорных обязательств.	3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	28 баллов, что соответствует Уровню риска 3	2	автоматизированное управление очередностью исполнения распоряжений Участников по времени поступления распоряжений; осуществление расчета в Системе до конца рабочего дня; выполнение Оператором ПС мониторинга объемов операций между Участниками, оперативный контроль резкого роста объемов операций того или иного Участника; разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев; установление доступного лимита Участнику, в пределах которого разрешается проведение операций перевода денежных средств или увеличение остатка электронных денежных средств соответственно; проведение расчетов в Платежной системе в пределах предоставленных Участниками денежных средств; контроль достаточности денежных средств на Счете ЦПКК; моментальное изменение Лимитов Участников и доступных Лимитов при авторизации операции перевода денежных средств, в том числе увеличения остатка электронных денежных средств по Распоряжениям Клиентов; контроль Оператором выполнения Участниками Временного регламента;	2
				нарушение внутренних процедур у Участников			1			2							
				сбои программно-аппаратных средств			4			2							
				концентрация значительного объема расчетных документов в определенные моменты и (или) периоды времени в течение дня			1			1							
				отзыв лицензии			2			4							
				введение ограничений на операции			3			2							

																иные способы управления рисками, в том числе: анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС) и (или) увеличение интервалов расчетов (несколько раз в день)	
1.2.	**Расчетный**	Отсутствие у Участников и (или) у ЦПКК денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами Платежной системы (риск ликвидности)	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	недостаточность (отсутствие) средств у Участника или у нескольких Участников, и (или) у ЦПКК, для своевременного выполнения ими своих расчетных обязательств перед другими Участниками (в том числе являющимися участником или расчетным центром платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие) и Оператором	Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.)	ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	1	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения процедуры приема к исполнению распоряжений Участников невозможность исполнения распоряжений ПКЦ о проведении расчетов с Участниками; возникновение дебиторской задолженности; нарушение договорных обязательств.	4	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	23 балла, что соответствует Уровню риска 3	2	выполнение Участниками ПС и (или) ЦПКК требований по финансовому обеспечению расчетов в ПС, контроль Оператором ПС лимитов авторизации Участников ПС; установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ; контроль достаточности денежных средств на счете ЦПКК; анализ и изучение финансовой отчетности, других сведений и документов Участников, ОУПИ (при их наличии); осуществление расчета в пределах предоставленных Участниками денежных средств; возможность блокирования в случае угрозы возникновения риска Оператором ПС операций между Участниками; внедрение процедур дополнительного контроля соблюдения сотрудниками регламентных процедур.	1
				финансовая несостоятельность РЦ и(или) Участника, и (или) ЦПКК;			1			3							
				концентрация значительного объема расчетных документов в определенные моменты и (или) периоды времени в течение дня			1			1							
				высокорисковая политика работы Участника или ЦПКК;			2			3							
				ошибки сотрудников (занимающихся распределением потоков (в РЦ) и пополнением корсчетов (у Участников и ЦПКК)			3			3							

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, *(P) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события, *(I) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которые влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска (R) *(согласно пп. 3.3.1, 4.1 Приложения №8 к Правилам,* $R = \Sigma Pi*Ii$, *при i=1…n, n - кол-во источников риск-события)*	Уровень допустимого риска *(в соответствии с п. 4.2 Приложения №8 к Правилам)*	Применяемые способы управления рисками	Уровень остаточного риска, (RR) *(рассчитывается аналогично уровню присущего риска после применения способов управления рисками согласно п. 6.1 Приложения №8 к Правилам)*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1.1.	**Правовой**	Претензии правового характера к Субъектам ПС со стороны государственных органов власти, ЦБ РФ	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	несоблюдение Субъектами ПС требований законодательства Российской Федерации	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	2	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения или задержка исполнения каждого Бизнес-процесса	5	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	25 баллов, что соответствует Уровню риска 3	2	предварительная проверка Оператором ПС потенциальных Участников ПС и ОУПИ на обладание необходимой правоспособностью (в соответствии с Правилами Платежной системы); мониторинг Оператором ПС информации об Участниках ПС и ОУПИ в открытых ресурсах, либо периодическая, не реже одного раза в год, выборочная проверка Оператором ПС Участников ПС и ОУПИ на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров; организация оперативного процесса подготовки/внесения изменений, согласования и утверждения ВНД Организации, в рамках меняющейся инфраструктуры ПС, требований регулятора и/или вводом в действие новых законопроектов;	2
				наличие правовых коллизий, и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России			3			3							
				неверное толкование положений нормативных актов и документов Оператора ПС			2			3							

					Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)							Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				дополнительный (внеплановый) анализ и изучение финансовой отчетности, других сведений и документов Участников ПС, ОУПИ, в случае появления негативной информации в СМИ об Участниках и/или ОУПИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС): а) осуществление расчета в пределах предоставленных Участниками денежных средств; б) автоматизированное управление очередностью исполнения распоряжений Участников ПС - по времени поступления распоряжений; в) осуществление расчета в Системе до конца рабочего дня; г) установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска. Также рекомендации п.10.4 Приложения №9 к Правилам	
1.2.	**Правовой**	Претензии правового характера к Субъектам ПС со стороны других Субъектов ПС, клиентов Участников ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	несоблюдение Субъектами ПС Правил ПС, заключенных договоров, документов Оператора ПС или Операторов УПИ	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	3	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения или задержка исполнения каждого Бизнес-процесса нарушение договорных обязательств	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	13 баллов, что соответствует Уровню риска 3	2	мониторинг Оператором ПС информации об Участниках ПС и ОУПИ в открытых ресурсах, либо 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	1

				несоблюдение Субъектами ПС внутренних документов, регламентирующих их деятельность в ПС	Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)		2			2		Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				деятельности и документов, в том числе внутренних документов и договоров; организация оперативного процесса подготовки/внесения изменений, согласования и утверждения ВНД Организации, в рамках меняющейся инфраструктуры ПС, требований регулятора и/или вводом в действие новых законопроектов; дополнительный (внеплановый) анализ и изучение финансовой отчетности, других сведений и документов Участников ПС, ОУПИ, в случае появления негативной информации в СМИ об Участниках ПС и/или ОУПИ, отслеживание и фиксирование параметров их работы в Системе; мероприятия, связанные с претензионной работой, которые указывают на необходимость соблюдения условий договоров, регламентов.	
				наличие недостатков внутренних документов Субъектов ПС			3			2							
1.3.	**Правовой**	Нахождение Оператора ПС, ОУПИ и Участников ПС под юрисдикцией различных государств	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица	изменение законодательства стран присутствия	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	2	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица	невозможность проведения или задержка исполнения каждого Бизнес-процесса нарушение	2	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	20 баллов, что соответствует Уровню риска 3	2	сбор информации от ответственных сотрудников Участников ПС нерезидентов; самостоятельный сбор информации о законодательстве	2

			вероятности и последствий.	различные подходы применимого сторонами законодательства, регулирующего порядок осуществления переводов денежных средств и связанных с ними процессов (например, идентификация, лимиты и т.п)	распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)		2	вероятности и последствий.	договорных обязательств	2		распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				стран присутствия; внесение изменений в бизнес-процессы и регламентную документацию.	
				санкции в отношении ОУПИ, Участников из определенной страны			4			3							

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, *(P) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события, *(I) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которые влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска (R) *(согласно пп. 3.3.1, 4.1 Приложения №8 к Правилам,* **R = Σ Pi*Ii,** *при i=1…n, n - кол-во источников риск-события*)	Уровень допустимого риска *(в соответствии с п. 4.2 Приложения №8 к Правилам)*	Применяемые способы управления рисками	Уровень остаточного риска, (RR) *(рассчитывается аналогично уровню присущего риска после применения способов управления рисками согласно п. 6.1 Приложения №8 к Правилам)*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1.1.	**Общий коммерческий**	Ухудшение финансового состояния Оператора ПС и (или) ОУПИ, не связанного с реализацией кредитного риска и риска ликвидности ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	потеря деловой репутации	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	сокращение дохода ПС	3	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	17 баллов, что соответствует Уровню риска 3	2	поддержание положительной деловой репутации Субъектов ПС; выполнение требований законодательных, нормативных документов, Правил, договоров; использование современного технологического обеспечения и технических средств; дополнительные меры, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС): - 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 уровня риска. контроль достаточности денежных средств на счете ЦПКК; поддержание уровня осведомленности об усугах, предоставляемых конкурентами; своевременный пересмотр текущей стратегии; поддержание и расширение клиентской базы.	1
				потеря конкурентноспособности			1			3							
				сокращение количества Участников и Клиентов, в том числе вследствие внешних факторов (форс-мажорные ситуации)			2			3							
				использование устаревших программно-аппаратных средств и технологий			1			2							
				неверная стратегия развития Оператора ПС или РЦ			1			3							

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, *(P) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события, *(I) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которые влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска (R) *(согласно пп. 3.3.1, 4.1 Приложения №8 к Правилам,* **R = ∑ Pi*Ii,** *при i=1…n, n - кол-во источников риск-события***)**	Уровень допустимого риска *(в соответствии с п. 4.2 Приложения №8 к Правилам)*	Применяемые способы управления рисками	Уровень остаточного риска, (RR) *(рассчитывается аналогично уровню присущего риска после применения способов управления рисками согласно п. 6.1 Приложения №8 к Правилам)*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1.1.	**Системный**	Распространение между Субъектами ПС последствий сочетания **двух** основных рисков, указанныхв пп. 1.2 - 1.5 Приложения 8 Правил, вызывающих нарушения функционирования ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	реализация одновременно двух основных рисков, указанных в пп. 1.2 - 1.5 Приложения 8 Правил	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	от 1 до 5 баллов	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	последствия одновременно двух основных рисков, указанных в пп. 1.2 - 1.5 Приложения 8 Правил	от 1 до 5 баллов	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	<=6	4	совокупность способов управления рисками, предусмотренных для операционного, расчетного, правового и общего коммерческого рисков.	<=4

					Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)							Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)					
1.2	**Системный**	Распространение между Субъектами ПС последствий сочетания нескольких (более двух) основных рисков, указанных в пп. 1.2 - 1.5 Приложения 8 Правил, 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 в пп. 1.2 - 1.5 Приложения 8 Правил	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников/ЦПКК в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК, Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	от 1 до 5 баллов	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы		от 1 до 5 баллов	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников/ЦПКК в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК, Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	>8	8	совокупность способов управления рисками, предусмотренных для операционного, расчетного, правового и общего коммерческого рисков.	<=8

Приложение №12 к Правилам Платежной системы МАРЛИН

ПРОФИЛЬ РИСКА НАРУШЕНИЯ БФПС

№	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, *(P) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события, *(I) (в баллах, согласно п. 3.3.5 Приложения №8 к Правилам)*	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которые влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска (R) *(согласно пп. 3.3.1, 4.1 Приложения №8 к Правилам,* $R = \Sigma Pi*Ii$, *при i=1…n, n - кол-во источников риск-события)*	Уровень допустимого риска *(в соответствии с п. 4.2 Приложения №8 к Правилам)*	Применяемые способы управления рисками	Уровень остаточного риска, (RR) *(рассчитывается аналогично уровню присущего риска после применения способов управления рисками согласно п. 6.1 Приложения №8 к Правилам)*
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1.1.	**Операционный**	Нарушение работоспособности аппаратно-программных комплексов Оператора ПС и/или Субъектов ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	возникновение сбоев, отказов и аварий в работе информационных и технологических систем, оборудования нарушения в каналах связи, электричества недостатки в организации и выполнении технологических и управленческих процессов	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и/или ЦПКК	4 2 1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность или задержка каждого Бизнес-процесса некорректное исполнение Бизнес-процесса 1.1. нарушение договорных обязательств влияние на значения	3 1 2	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и/или ЦПКК	24 балла, что соответствует Уровню риска 3	2	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;	1

				использование устаревших программно-аппаратных средств и технологий	поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК, Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)		1		показателей БФПС.	2		поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				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; 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.	
				ошибки или противоправные действия персонала Оператора ПС и/или Субъектов ПС			2			3								
1.2.	**Операционный**	Нарушение сроков выполнения Временного регламента Оператором ПС и/или Субъектами ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	возникновение сбоев, отказов и аварий в работе информационных и технологических систем, оборудования	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность или задержка каждого Бизнес-процесса нарушение договорных обязательств влияние на значения показателей БФПС.	3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	14 баллов, что соответствует Уровню риска 3	2	регламентирование порядка выполнения основных процессов в ПС в Правилах; регламентирование порядка совершения операций в рамках Правил и 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	1
				нарушения в каналах связи, электричества			2			1								
				недостатки в организации и выполнении технологических и управленческих процессов			1			2								

				ошибки или противоправные действия персонала Оператора ПС и/или Субъектов ПС	поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК, Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)		1			1		поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				совершением операций, установление ограничений на сроки и объемы операций; разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев; 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.	
1.3.	**Операционный**	Воздействие событий, причины возникновения которых не связаны с деятельностью Оператора ПС и/или Субъекто в ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	чрезвычайные ситуации	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и/или ЦПКК	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность или задержка каждого Бизнес-процесса нарушение договорных обязательств влияние на значения показателей БФПС.	3	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	24 балла, что соответствует Уровню риска 3	2	создание необходимых организационных и технических условий для обеспечения БФПС при совершении операций (на случай аварий, пожаров, терактов и других непредвиденных ситуаций); разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев; поиск новых направлений развития	1
				обстоятельства непреодолимой силы , в том числе политические внешнеэкономические факторы			3			5								
				ошибочные действия третьих лиц (физических и юридических)			1			3								
				противоправные действия третьих лиц (физических и юридических).			1			3								

					в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)							Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)					
1.4.	**Операционный**	Нарушение порядка обеспечения защиты информации	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	ошибки или противоправные действия персонала Оператора ПС и/или Субъектов ПС	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и/или ЦПКК	3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность или задержка каждого Бизнес-процесса нарушение договорных обязательств влияние на значения показателей БФПС.	4	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	27 баллов, что соответствует Уровню риска 3	2	обеспечение информационной безопасности; контроль над доступом к информации; применение многоуровневой защиты информации с использованием сертифицированных средств защиты информации; регламентирование процессов защиты информации; применение принципов разделения и ограничения функций в целях определения предела полномочий сотрудников, осуществляющих операции.	1
				недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации			1			3							
				недостатки прикладного программного обеспечения автоматизированных систем и приложений			3			3							
				несоблюдение требований к указанным процессам деятельности операторами по переводу денежных средств, являющимися Участниками Системы, Операторами УПИ			1			3							

1.5.	Операционный	Нарушение работоспособности систем и сервисов, предоставляемых привлеченными поставщиками (провайдерами)	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	ошибки или противоправные действия персонала Оператора ПС и/или Субъектов ПС	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и/или ЦПКК	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	невозможность или задержка каждого Бизнес-процесса нарушение договорных обязательств влияние на значения показателей БФПС	2	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и/или ЦПКК	15 баллов, что соответствует Уровню риска 3	2	проверка поставщика (провайдера) перед заключением договора анализ проекта договора на предмет наличия и содержания условий об уровне качества предоставляемых услуг (SLA) контроль качества предоставляемой услуги (выполняемых работ) 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 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	1
				нарушение договорных обязательств Оператором или поставщиком (провайдером)			2			2							
				нарушения функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, предоставляемого привлеченными поставщиками (провайдерами)			3			3							
2.1.	Расчетный	Невыполнение Участниками договорных обязательств перед РЦ и (или) ЦПКК в установленный срок или в будущем (кредитный риск)	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	недостаточность (отсутствие) средств у Участника или у нескольких Участников, для своевременного выполнения ими своих расчетных обязательств РЦ и (или) ЦПКК платежной системы, с которым Оператор Системы осуществляет межсистемное взаимодействие	Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.)	ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	1	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения процедуры приема к исполнению распоряжений Участников невозможность исполнения распоряжений ПКЦ и (или)	3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	28 баллов, что соответствует Уровню риска 3	2	автоматизированное управление очередностью исполнения распоряжений Участников по времени поступления распоряжений; осуществление расчета в Системе до конца рабочего дня; выполнение Оператором ПС мониторинга объемов операций между Участниками, оперативный контроль резкого роста объемов операций того или иного Участника; разработка, поддержание в актуальном состоянии планов обеспечения непрерывности	2

				нарушение внутренних процедур у Участников			1		ЦПКК о проведении расчетов с Участниками; возникновение дебиторской задолженности; нарушение договорных обязательств.	2		ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				деятельности и восстановления деятельности после сбоев; установление доступного лимита Участнику, в пределах которого разрешается проведение операций перевода денежных средств или увеличение остатка электронных денежных средств соответственно; проведение расчетов в Платежной системе в пределах предоставленных Участниками денежных средств; контроль достаточности денежных средств на Счете ЦПКК; моментальное изменение Лимитов Участников и доступных Лимитов при авторизации операции перевода денежных средств, в том числе увеличения остатка электронных денежных средств по Распоряжениям Клиентов; контроль Оператором выполнения Участниками Временного регламента; иные способы управления рисками, в том числе: анализ и изучение информации в СМИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС) и (или) увеличение интервалов расчетов (несколько раз в день)	
				сбои программно-аппаратных средств			4			2							
				концентрация значительного объема расчетных документов в определенные моменты и (или) периоды времени в течение дня			1			1							
				отзыв лицензии			2			4							
				введение ограничений на операции			3			2							
2.2.	**Расчетный**	Отсутствие у Участников и (или) у ЦПКК денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъекта	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	недостаточность (отсутствие) средств у Участника или у нескольких Участников, и (или) у ЦПКК, для своевременного выполнения ими своих расчетных обязательств перед другими Участниками (в том числе являющимися участником или расчетным центром	Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.)	ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	1	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения процедуры приема к исполнению распоряжений Участников невозможность исполнения распоряжений	4	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Передача обработанных распоряжений Участников/ЦПКК в РЦ	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	23 балла, что соответствует Уровню риска 3	2	выполнение Участниками ПС и (или) ЦПКК требований по финансовому обеспечению расчетов в ПС, контроль Оператором ПС лимитов авторизации Участников ПС; установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ; контроль достаточности денежных средств на счете ЦПКК; анализ и изучение финансовой отчетности,	1

		ми Платежной системы (риск ликвидности)		платежной системы, с которой Оператор Системы осуществляет межсистемное взаимодействие) и Оператором					ПКЦ о проведении расчетов с Участниками;			(2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				других сведений и документов Участников, ОУПИ (при их наличии); осуществление расчета в пределах предоставленных Участниками денежных средств;	
				финансовая несостоятельность РЦ и(или) Участника, и (или) ЦПКК;			1		возникновение дебиторской задолженности;	3						возможность блокирования в случае угрозы возникновения риска Оператором ПС операций между Участниками; внедрение процедур дополнительного контроля соблюдения сотрудниками регламентных процедур.	
				концентрация значительного объема расчетных документов в определенные моменты и (или) периоды времени в течение дня			1		нарушение договорных обязательств.	1							
				высокорисковая политика работы Участника или ЦПКК;			2			3								
				ошибки сотрудников (занимающихся распределением потоков (в РЦ) и пополнением корсчетов (у Участников и ЦПКК)			3			3								
3.1.	**Правовой**	Претензии правового характера к Субъектам ПС со стороны государственных органов власти, ЦБ РФ	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	несоблюдение Субъектами ПС требований законодательства Российской Федерации	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	2	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения или задержка исполнения каждого Бизнес-процесса нарушение договорных обязательств	5	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	25 баллов, что соответствует Уровню риска 3	2	предварительная проверка Оператором ПС потенциальных Участников ПС и ОУПИ на обладание необходимой правоспособностью (в соответствии с Правилами Платежной системы);	2
				наличие правовых коллизий, и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России			3			3						мониторинг Оператором ПС информации об Участниках ПС и ОУПИ в открытых ресурсах, либо периодическая, не реже одного раза в год, выборочная проверка Оператором ПС Участников ПС и ОУПИ на обладание необходимой правоспособностью путем запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров;	
																	организация оперативного	

				неверное толкование положений нормативных актов и документов Оператора ПС	распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)		2			3		распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				процесса подготовки/внесения изменений, согласования и утверждения ВНД Организации, в рамках меняющейся инфраструктуры ПС, требований регулятора и/или вводом в действие новых законопроектов; дополнительный (внеплановый) анализ и изучение финансовой отчетности, других сведений и документов Участников ПС, ОУПИ, в случае появления негативной информации в СМИ об Участниках и/или ОУПИ, отслеживание и фиксирование параметров их работы в Системе, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС): а) осуществление расчета в пределах предоставленных Участниками денежных средств; б) автоматизированное управление очередностью исполнения распоряжений Участников ПС - по времени поступления распоряжений; в) осуществление расчета в Системе до конца рабочего дня; г) установление предельных размеров (лимитов) обязательств в отношении Участников, открывших счета в привлеченном РЦ, с учетом уровня риска. Также рекомендации п.10.4 Приложения №9 к Правилам	
3.2.	**Правовой**	Претензии правового характера к Субъектам ПС со стороны других Субъектов ПС, клиентов Участников ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и	несоблюдение Субъектами ПС Правил ПС, заключенных договоров, документов Оператора ПС или Операторов УПИ	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и)	3	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения или задержка исполнения каждого Бизнес-процесса нарушение договорных	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и)	13 баллов, что соответствует Уровню риска 3	2	мониторинг Оператором ПС информации об Участниках ПС и ОУПИ в открытых ресурсах, либо 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	1

			последствий.	несоблюдение Субъектами ПС внутренних документов, регламентирующих их деятельность в ПС наличие недостатков внутренних документов Субъектов ПС	Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)		2 3		обязательств	2 2		Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)				договоров; организация оперативного процесса подготовки/внесения изменений, согласования и утверждения ВНД Организации, в рамках меняющейся инфраструктуры ПС, требований регулятора и/или вводом в действие новых законопроектов; дополнительный (внеплановый) анализ и изучение финансовой отчетности, других сведений и документов Участников ПС, ОУПИ, в случае появления негативной информации в СМИ об Участниках ПС и/или ОУПИ, отслеживание и фиксирование параметров их работы в Системе; мероприятия, связанные с претензионной работой, которые указывают на необходимость соблюдения условий договоров, регламентов.	
3.3.	**Правовой**	Нахождение Оператора ПС, ОУПИ и Участников ПС под юрисдикцией различных государств	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	изменение законодательства стран присутствия различные подходы применимого сторонами законодательства, регулирующего порядок осуществления переводов денежных средств и связанных с ними процессов (например, идентификация, лимиты и т.п) санкции в отношении ОУПИ, Участников из определенной страны	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	2 2 4	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	невозможность проведения или задержка исполнения каждого Бизнес-процесса нарушение договорных обязательств	2 2 3	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	20 баллов, что соответствует Уровню риска 3	2	сбор информации от ответственных сотрудников Участников ПС нерезидентов; самостоятельный сбор информации о законодательстве стран присутствия; внесение изменений в бизнес-процессы и регламентную документацию.	2

					и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)							Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)					
4.1.	**Общий коммерческий**	Ухудшение финансового состояния Оператора ПС и (или) ОУПИ, не связанного с реализацией кредитного риска и риска ликвидности ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	потеря деловой репутации	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	1	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	сокращение дохода ПС	3	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	17 баллов, что соответствует Уровню риска 3	2	поддержание положительной деловой репутации Субъектов ПС; выполнение требований законодательных, нормативных документов, Правил, договоров; использование современного технологического обеспечения и технических средств; дополнительные меры, в т.ч. соблюдение порядка расчетов (согласно Правилам ПС): - 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 уровня риска. контроль достаточности денежных средств на счете ЦПКК; поддержание уровня осведомленности об усугах, предоставляемых конкурентами; своевременный пересмотр текущей стратегии; поддержание и расширение клиентской базы.	1
				потеря конкурентноспособности			1			3								
				сокращение количества Участников и Клиентов, в том числе вследствие внешних факторов (форс-мажорные ситуации)			2			3								
				использование устаревших программно-аппаратных средств и технологий			1			2								
				неверная стратегия развития Оператора ПС или РЦ			1			3								

5.1.	**Системный**	Распространение между Субъектами ПС последствий сочетания **двух** основных рисков, указанных в пп. 1.2 - 1.5 Приложения 8 Правил, вызывающих нарушения функционирования ПС	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	реализация одновременно двух основных рисков, указанных в пп. 1.2 - 1.5 Приложения 8 Правил	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	от 1 до 5 баллов	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	последствия одновременно двух основных рисков, указанных в пп. 1.2 - 1.5 Приложения 8 Правил	от 1 до 5 баллов	Метод номинальной группы. Сценарный анализ с использованием статистических данных. Матрица вероятности и последствий.	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	<=6	4	совокупность способов управления рисками, предусмотренных для операционного, расчетного, правового и общего коммерческого рисков.	<=4

5.2.	**Системный**	Распространение между Субъектами ПС последствий сочетания нескольких (более двух) основных рисков, указанных в пп. 1.2 - 1.5 Приложения 8 Правил, 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 в пп. 1.2 - 1.5 Приложения 8 Правил	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников/ЦПКК в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК, Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник (и) и (или) ЦПКК	от 1 до 5 баллов	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы		от 1 до 5 баллов	Метод индексов риска и элементы методик, основанных на статистическом и сценарном анализе функционирования системы	Проверка возможности осуществления операций: Прием и обработка распоряжений Участников, Передача подтверждений о приеме и обработке распоряжений или об отказе в приеме и обработке распоряжений Участников (1.1.) и/или Передача обработанных распоряжений Участников/ЦПКК в ПКЦ (1.2.) и/или Прием распоряжений, поступивших из ОЦ (2.1.) и/или Процедуры приема к исполнению распоряжений Участников/ЦПКК (контроль поступивших распоряжений) (2.2.) и/или Прием к исполнению распоряжений Участников/ЦПКК при положительном результате процедур контроля поступивших распоряжений или об отказе в приеме распоряжений к исполнению (2.3.) и/или Направление извещений об обработанных и об исполненных распоряжениях Участникам/ЦПКК, Передача обработанных распоряжений Участников/ЦПКК в РЦ (2.4.) и/или Исполнение распоряжений ПКЦ о проведении расчетов с Участниками/ЦПКК (3.1.) и/или Направление подтверждений в ПКЦ о проведении расчетов с Участниками/ЦПКК (3.2.)	Оператор ПС и/или ОЦ и/или ПКЦ и/или РЦ и/или Участник(и) и (или) ЦПКК	>8	8	совокупность способов управления рисками, предусмотренных для операционного, расчетного, правового и общего коммерческого рисков.	<=8