

Приложение
УТВЕРЖДЕНО
приказом ООО «СПС» от 26 декабря 2023 года № 72

**Положение
об организации управления рисками и обеспечения
бесперебойности функционирования
Страховой платежной системы**

редакция № 11

Москва

Оглавление

1. ОБЩИЕ ПОЛОЖЕНИЯ.....	4
2. ТЕРМИНЫ И СОКРАЩЕНИЯ	5
3. ТРЕБОВАНИЯ К ПОРЯДКУ ОБЕСПЕЧЕНИЯ БФПС, ПОКАЗАТЕЛЯМ БФПС	7
4. ПОКАЗАТЕЛИ БФПС.....	17
5. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ СИСТЕМЫ ПО ОБЕСПЕЧЕНИЮ БФПС С УЧЕТОМ ОРГАНИЗАЦИОННОЙ МОДЕЛИ УПРАВЛЕНИЯ РИСКАМИ.....	30
6. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ОПЕРАТОРАМИ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ И УЧАСТНИКАМИ СТРАХОВОЙ ПЛАТЕЖНОЙ СИСТЕМЫ ПОРЯДКА ОБЕСПЕЧЕНИЯ БФПС.....	33
7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.....	34
Приложение № 1	35
Приложение № 2	37
Приложение № 3	38
Приложение № 4	40
Таблица 1	44
Таблица 2	48
Таблица 3	49
Таблица 4	50
Приложение № 5	51

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Положение об организации управления рисками и обеспечения бесперебойности функционирования Страховой платежной системы (далее – Положение) разработано в соответствии с:

- Федеральным законом от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – ФЗ № 161-ФЗ);
- Положением 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);
- Указанием Банка России от 9 января 2023 № 6352-У «О внесении изменений в Положение 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»;
- Указанием Банка России от 11 июня 2014 года № 3280-У «О порядке информирования оператором платежной системы Банка России, участников платежной системы о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры» (далее – Указание Банка России № 3280-У);
- ГОСТ Р 58771-2019 «Национальный стандарт Российской Федерации. Менеджмент риска. Технологии оценки риска», утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2019 года № 1405-ст (далее – Стандарт).

1.2. Требования Положения применяются к Оператору Системы, Операторам услуг платежной инфраструктуры, а также Участникам при

обеспечении ими бесперебойности функционирования Страховой платежной системы как способности предупреждать нарушения требований действующего законодательства Российской Федерации, Правил Страховой платежной системы, заключенных договоров.

1.3. Во всем остальном, что не урегулировано Положением, Субъекты системы руководствуются действующим законодательством Российской Федерации, нормативными актами Банка России, Правилами Страховой платежной системы.

2. ТЕРМИНЫ И СОКРАЩЕНИЯ

2.1. Термины и определения, используемые по тексту Положения, имеют значение и толкуются в соответствии с их значениями, содержащимися в Правилах Страховой платежной системы, утвержденных Генеральным директором ООО «СПС» 21 декабря 2012 года, в Положении Банка России № 607-П, а в случае отсутствия соответствующего толкования в вышеуказанных документах – в соответствии с действующим законодательством Российской Федерации, в том числе ФЗ № 161-ФЗ.

2.2. Дополнительно в тексте Положения используются следующие понятия:

БФПС – бесперебойность функционирования Страховой платежной системы.

Операторы услуг платежной инфраструктуры (ОУПИ) – Операционный центр, Платежный клиринговый центр, Расчетный центр.

Участник-Банк (Оператор по переводу денежных средств, ОПДС) – кредитная организация, которая в соответствии с действующим законодательством Российской Федерации вправе осуществлять перевод денежных средств, присоединившаяся к Правилам Страховой платежной системы.

Бизнес-процесс – один или несколько процессов, в рамках которых обеспечивается оказание услуг платежной инфраструктуры Операционным центром, Платежным клиринговым центром и Расчетным центром.

Инцидент¹ – событие в Страховой Платежной системе, которое привело к нарушению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств, в результате которого приостанавливалось оказание услуг платежной инфраструктуры.

Инцидент информационной безопасности (Инцидент ИБ) – событие информационной безопасности, связанное с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, к которому относятся:

- события, которые привели или могут привести к осуществлению переводов денежных средств без согласия клиента (Участника-Страховщика);
- события, которые привели или могут привести к неоказанию услуг платежной инфраструктуры;
- события, 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 информационно-телекоммуникационной сети «Интернет».

Риск-событие – событие в Страховой платежной системе, отрицательное последствие которого может привести к возникновению Инцидента.

Риск-событие информационной безопасности (Риск-событие ИБ) – событие в Страховой платежной системе, отрицательное последствие которого может привести к возникновению Инцидента ИБ.

Значимый риск – риск, для которого уровень присущего риска до применения способов управления рисками в Страховой платежной системе может превысить или превысил уровень допустимого риска.

¹ Прекращение участия в Страховой платежной системе в случаях, предусмотренных Правилами Страховой платежной системы в соответствии с пунктом 4 части 1 статьи 20 Федерального закона от 27 июня 2011 года № 161- ФЗ «О национальной платежной системе», не рассматривается в качестве инцидентов.

Уровень допустимого риска – максимальный уровень риска, при котором восстановление оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, включая восстановление оказания услуг платежной инфраструктуры в случае приостановления их оказания, осуществляется в течение периодов времени, установленных Оператором Системы, и предполагаемый ущерб от которого Оператор Системы готов принять без применения способов управления рисками в Страховой платежной системе.

Уровень остаточного риска – уровень каждого из значимых для Страховой платежной системы рисков после применения способов управления рисками в Системе.

Уровень присущего риска – уровень риска, имеющийся до применения способов управления рисками в Страховой платежной системе.

Уровень риска – величина риска, характеризуемая вероятностью наступления Риск-события и величиной возможных последствий его реализации.

3. ТРЕБОВАНИЯ К ПОРЯДКУ ОБЕСПЕЧЕНИЯ БФПС, ПОКАЗАТЕЛЯМ БФПС

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

– по организации системы управления рисками в Страховой платежной системе, оценке и управлению рисками (далее при совместном упоминании – управление рисками в Страховой платежной системе);

– по выявлению оказания услуг платежной инфраструктуры, не соответствующего требованиям к оказанию услуг, обеспечению функционирования Страховой платежной системы в случае нарушения оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, и восстановлению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, включая восстановление оказания услуг платежной инфраструктуры в случае приостановления их оказания в течение периодов времени, установленных Оператором Системы в Правилах

Страховой платежной системы (далее при совместном упоминании – управление непрерывностью функционирования Страховой платежной системы).

3.2. Основными этапами управления рисками являются:

- идентификация риска – выявление риска, определение причин и предпосылок его возникновения;
- анализ и оценка риска – анализ информации, полученной в результате идентификации риска, определение вероятности наступления негативных для Страховой платежной системы последствий;
- разработка и проведение мероприятий по ограничению, снижению, предупреждению риска;
- мониторинг уровня риска – анализ риска в динамике его развития;
- принятие мер по устранению повышенного риска и его последствий.

3.3. Оператор Системы управляет рисками в Страховой платежной системе с учетом следующего:

- организовывает систему управления рисками с учетом организационной модели управления рисками, определенной пунктом 5.1 Правил Страховой платежной системы;
- применяет способы управления рисками в Страховой платежной системе, определенные в пункте 5.3 Правил Страховой платежной системы.

3.4. Характеристики БФПС:

- а) оказание услуг платежной инфраструктуры Участникам в соответствии с требованиями;
- б) способность восстанавливать оказание услуг платежной инфраструктуры в случае их приостановления (прекращения) за установленный период времени;
- в) способность восстанавливать оказание услуг платежной инфраструктуры в соответствии с требованиями в случае нарушения требований (даже без приостановления) за установленный период времени.

3.5. Требования к оказанию услуг платежной инфраструктуры установлены:

- ФЗ № 161-ФЗ;

- принятymi в соответствии с ФЗ № 161-ФЗ нормативными актами Банка России;
- положениями Правил Страховой платежной системы;
- положениями договоров об оказании услуг платежной инфраструктуры;
- положениями внутренних документов Оператора Системы.

3.6. Основными рисками, которые могут привести к нарушению БФПС в Страховой платежной системе, принимаются следующие виды рисков:

- правовой риск;
- операционный риск (включая риск информационной безопасности);
- кредитный риск;
- риск ликвидности;
- общий коммерческий риск;
- системный риск.

3.6.1. Причины возникновения и источники Риск-событий правового риска в Страховой платежной системе связаны:

- с несоблюдением Субъектами системы требований действующего законодательства Российской Федерации, Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и документов ОУПИ;
- с наличием правовых коллизий и (или) правовой неопределенности в действующем законодательстве Российской Федерации, нормативных актах Банка России, Правилах Страховой платежной системы и договорах, заключенных между Субъектами системы.

Общие принципы управления правовым риском состоят в применении Оператором Системы следующих мер:

- предварительная проверка потенциальных Участников и Расчетного центра на обладание необходимой правоспособностью в рамках действующего законодательства Российской Федерации;
- мониторинг действующего законодательства Российской Федерации и

нормативных актов Банка России;

- контроль соответствия документов Оператора Системы действующему законодательству Российской Федерации о национальной платежной системе;
- анализ факторов возникновения правовых рисков: рассматриваются и изучаются вопросы, жалобы и претензии Участников;
- наличие детализированных Правил Страховой платежной системы, позволяющих ее Участникам однозначно определять свои права и обязанности;
- установление эффективной структуры договорных отношений в Страховой платежной системе;
- наличие типовых договоров банковских счетов, заключаемых между Расчетным центром и Участниками;
- наличие установленных требований к договору банковского счета (счета гарантиного фонда), на основании которого Участнику-Страховщику открывается Счет (Счета) гарантиного фонда Страховой платежной системы;
- обеспечение возможности досудебного рассмотрения споров между Субъектами системы.

Выявление и оценка правовых рисков осуществляется Оператором Системы на постоянной основе.

3.6.2. Причины возникновения и источники Риск-событий операционного риска, включая Риск-события ИБ, в Страховой платежной системе связаны с:

- возникновением финансовых потерь (убытков), способных повлиять на БФПС, в результате несоответствия характера и масштаба деятельности Страховой платежной системы требованиям действующего законодательства Российской Федерации, Правилам Страховой платежной системы, внутренним регламентам взаимодействия структурных подразделений Оператора Системы, их нарушениями работниками Оператора Системы (вследствие непреднамеренных или умышленных действий, или бездействий работников);
- несоразмерностью (недостаточностью) функциональных возможностей (характеристик) применяемых в Страховой платежной системе

информационных, технологических и других систем и (или) их отказов (нарушений функционирования);

– нарушением информационной безопасности на различных уровнях, а именно: на физическом уровне информационной инфраструктуры, на уровне сетевого оборудования, на уровне сетевых приложений и сервисов, на уровне операционных систем;

– ненадлежащим обеспечением защиты информации в результате недостатков процессов обеспечения защиты информации, в том числе недостатков применяемых технологических мер защиты информации, недостатков прикладного программного обеспечения автоматизированных систем и приложений, а также несоблюдением требований к указанным процессам деятельности ОПДС и ОУПИ;

– отсутствием технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры Страховой платежной системы (далее – технические средства защиты информации от воздействия вредоносного кода), на средствах вычислительной техники;

– нерегулярным обновлением версий технических средств защиты информации от воздействия вредоносного кода и баз данных, используемых в работе технических средств защиты информации от воздействия вредоносного кода и содержащих описание вредоносных кодов и способы их обезвреживания;

– ненадлежащим обеспечением функционирования технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме и проведения предварительной проверки на отсутствие вредоносного кода программного обеспечения (устанавливаемого или изменяемого), используемого в Страховой платежной системе.

Общие принципы управления операционным риском, включая риск информационной безопасности, состоят в применении Оператором Системы следующих мер:

- регламентирование порядка выполнения основных процессов и процедур в Правилах Страховой платежной системы, договорах об оказании услуг платежного клиринга и внутренних документах Оператора Системы;
- автоматизация проведения операций;
- снижение рисков, связанных с персоналом, путем ограничения функций и полномочий сотрудников;
- фиксация и обработка информации о фактах нарушения нормальной работы структурных подразделений, штатной работы программно-технических средств, правил и требований к совершению операций, которые могли привести (привели) к расходам (убыткам);
- дублирование подачи электропитания к вычислительному центру;
- использование дополнительных автономных источников электропитания (электрогенераторов);
- обязательное использование источников бесперебойного электропитания (далее – ИБП) на основе аккумуляторных батарей;
- оптимизация распределения нагрузок на ИБП для обеспечения максимальной продолжительности работы критичных сервисов;
- дублирование каналов связи и каналов информационного взаимодействия (далее – каналы), то есть обеспечение приема и обработки информации по нескольким каналам, а также представление отчетов о выполненных операциях, как по основному, так и по резервному каналу;
- обязательное резервирование используемых серверов;
- использование современных средств и методов повышения отказоустойчивости систем энергоснабжения, кондиционирования, пожаротушения, безопасности и других систем обеспечения безотказной работы средств электронного взаимодействия;
- проверка устанавливаемого программного обеспечения, как системного, так и прикладного, на этапе опытной эксплуатации до ввода в промышленную эксплуатацию;

- использование защищенных каналов передачи данных при использовании информационно-телекоммуникационной сети «Интернет»;
- построение процессов выявления и устранения уязвимостей информационной безопасности, а также оценки состояния информационной безопасности объектов информационной инфраструктуры;
- обеспечение требуемого уровня информационной безопасности в области защиты информации в соответствии с требованиями федеральных законов, нормативно-методическими документами Банка России, а также Федеральной службы безопасности России и Федеральной службы по техническому и экспортному контролю России;
- разработка и постоянная актуализация плана обеспечения непрерывности и восстановления деятельности (далее – план ОНиВД);
- блокирование источника вредоносного воздействия или кода;
- централизованное обновление антивирусных баз на серверах администрирования средств антивирусной защиты и всех объектов антивирусной защиты;
- переход на альтернативные каналы взаимодействия в Страховой платежной системе, не затронутые источником вредоносного воздействия;
- применение мер технического «лечения» Страховой платежной системы;
- приостановление переводов денежных средств в Страховой платежной системе, предусмотренных разделом 2 Правил Страховой платежной системы, в случаях, когда нарушение системы защиты в Страховой платежной системе, в том числе посредством распространения вредоносного кода, угрожает целостности Системы, способно нанести значительный ущерб Оператору Системы и/или Субъектам системы.

3.6.3. Причины возникновения и источники Риск-событий кредитного риска в Страховой платежной системе связаны с тем, что требования Участников-Страховщиков, возникающие у них по договорным обязательствам, не будут своевременно оплачены в рамках расчетной сессии по итогам платежного клиринга

из-за несоблюдения платежных и расчетных процессов, определенных в Страховой платежной системе.

Общие принципы управления кредитным риском состоят в применении Оператором Системы мер по контролю следующих процедур в соответствии с Правилами Страховой платежной системы:

- выполнение Участниками-Страховщиками требований по финансовому обеспечению расчетов в Страховой платежной системе;
- осуществление расчетов в Страховой платежной системе в пределах, предоставленных Участниками-Страховщиками денежных средств;
- выполнение мониторинга объемов операций между Участниками-Страховщиками, оперативный контроль того или иного Участника-Страховщика, исключение из расчетов части или всей суммы его обязательств.

3.6.4. Причины возникновения и источники Риск-событий риска ликвидности в Страховой платежной системе связаны с тем, что у Участника-Страховщика в Страховой платежной системе будет недостаточно денежных средств для своевременного выполнения принятых на себя финансовых обязательств перед другими Участниками в полной мере.

Общие принципы управления риском ликвидности состоят в применении Оператором Системы мер по контролю следующих процедур в соответствии с Правилами Страховой платежной системы и (или) договорами Страховой платежной системы:

- сумма доступного остатка денежных средств, находящихся на Счете Участника, открытого в Расчетном центре и предназначенного для расчета в Страховой платежной системе, по состоянию на 09 ч 00 мин дня открытия расчетной сессии должна быть не менее суммы его денежных обязательств;
- наличие минимального размера денежных средств на Счетах гарантийного фонда Платежной системы Участника-Страховщика, созданных для обеспечения исполнения его обязательств при осуществлении конкретного вида перевода денежных средств;
- мониторинг деятельности Участников-Банков в части соблюдения

критериев участия в Страховой платежной системе, в которых Участники-Страховщики размещают денежные средства для обеспечения расчетов в Страховой платежной системе.

3.6.5. Причины возникновения и источники Риск-событий общего коммерческого риска в Страховой платежной системе связаны с оказанием услуг платежной инфраструктуры, не соответствующего требованиям к оказанию услуг, вследствие ухудшения финансового состояния Оператора Системы и (или) ОУПИ, не связанного с реализацией кредитного риска и риска ликвидности, в том числе, из-за потери деловой репутации.

Общие принципы управления общим коммерческим риском включают использование современных технологий и поддержание положительной деловой репутации Страховой платежной системы. Также в целях минимизации данного вида риска Оператору Системы и ОУПИ, прежде всего Расчетному центру, необходимо обладать ликвидными чистыми активами, достаточными для продолжения деятельности.

3.6.6. Причины возникновения и источники Риск-событий системного риска в Страховой платежной системе связаны с оказанием услуг платежной инфраструктуры, не соответствующего требованиям к оказанию услуг, вследствие неспособности одного или нескольких Субъектов системы исполнить принятые на себя обязательства или нарушений в самой Страховой платежной системе, которые вызовут неспособность большинства или всех Субъектов системы исполнить свои обязательства в срок.

Системный риск может возникнуть как по финансовым причинам, так и вследствие сбоев в энергоснабжении, сетях связи или отказов оборудования, или недостатков программного обеспечения. Таким образом, возникновение системного риска является следствием возникновения одновременно нескольких, всех сразу, или одного из рисков, приведенных в пунктах 3.6.1 - 3.6.5 Положения.

В этой связи общие принципы управления системным риском в зависимости от причины его возникновения состоят в применении Оператором Системы мер, указанных в пунктах 3.6.1 - 3.6.5 Положения.

3.7. Оператор Системы в целях управления рисками в Страховой платежной системе разрабатывает методику анализа рисков в Страховой платежной системе, включая риск нарушения БФПС (Приложение № 4 к Положению).

Оператор Системы должен проводить плановую оценку рисков в Страховой платежной системе, а также внеплановые оценки рисков в Страховой платежной системе с использованием методик анализа рисков в Страховой платежной системе и составлением профилей рисков.

Оператор Системы должен проводить внеплановую оценку всех рисков в Страховой платежной системе при внесении изменений в один или несколько Бизнес-процессов. Проведение внеплановой оценки всех рисков в Страховой платежной системе должно быть завершено не позднее истечения 6 (шести) месяцев со дня внесения указанных изменений.

Оператор Системы должен проводить внеплановую оценку отдельных рисков (отдельного риска) в Страховой платежной системе в срок не позднее истечения 4 (четырех) месяцев со дня возникновения следующих событий:

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

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

Также Оператор Системы должен проводить внеплановую оценку отдельных

рисков (отдельного риска) в Страховой платежной системе в срок не позднее истечения 4 (четырех) месяцев со дня выявления Значимого риска в Страховой платежной системе, для которого уровень присущего риска до применения способов управления рисками в Страховой платежной системе может превысить или превысил уровень допустимого риска.

Плановая оценка всех рисков в Страховой платежной системе проводится Оператором Системы не реже 1 (одного) раза в 3 (три) года с учетом сведений о событиях, которые произошли в Страховой платежной системе со дня завершения предыдущей плановой или внеплановой оценки всех рисков в Страховой платежной системе и привели к приостановлению (прекращению) оказания услуг платежной инфраструктуры.

Результатом анализа рисков являются профили рисков (Приложение № 2 к Положению). Оператор Системы составляет профили рисков по всем Значимым рискам в Страховой платежной системе, а также пересматривает (актуализирует) их по результатам плановой или внеплановой оценки всех рисков в Страховой платежной системе, а также внеплановой оценки отдельных рисков (отдельного риска) в Страховой платежной системе.

Профиль риска нарушения БФПС должен составляться как сводный профиль в отношении всех Значимых рисков в Страховой платежной системе.

Оператор Системы хранит сведения, содержащиеся в профилях рисков, не менее 5 (пяти) лет со дня составления и пересмотра (актуализации) профилей рисков.

4. ПОКАЗАТЕЛИ БФПС

4.1. Оператор Системы должен определять следующие показатели БФПС:

№ п/п	Показатель БФПС	Пороговый уровень показателя БФПС	Категория Субъектов системы, влияющих на показатели БФПС	Порядок расчета показателя БФПС
			<p>Не более 6 часов*</p> <p>* Период времени, в течение которого должно восстановлено оказание услуг платежной инфраструктуры, соответствующее требованиям оказанию услуг, в случае нарушения указанных требований, соответствует пороговому значению показателя П1.</p>	<p>П1 = Т_{1'} – Т₁</p> <p>где:</p> <p>Т₁ – момент возникновения события, приведшего к приостановлению оказания услуг платежной инфраструктуры в результате первого из возникших Инцидентов;</p> <p>Т_{1'} – момент восстановления оказания услуг платежной инфраструктуры.</p> <p>При возникновении Инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры одновременно двумя и более ОУПИ показатель П1 должен рассчитываться как период времени с момента возникновения события, приведшего к приостановлению оказания услуг платежной инфраструктуры в результате первого из возникших Инцидентов, и до момента восстановления оказания услуг платежной инфраструктуры всеми ОУПИ, у которых возникили Инциденты.</p>

Категория Субъектов системы, влияющих на показатели БФПС				Порядок расчета показателя БФПС		
№ п/п	Показатель БФПС	Пороговый уровень показателя БФПС	Показатель	Показатель П1	Показатель П2	Показатель
				часах/минутах/секундах.	в часах/минутах/секундах.	
2.	Показатель непрерывности оказания услуг платежной инфраструктуры П2	Не менее 72 часов				
3.	Показатель соблюдения ПЗ регламента П3	Не менее 98,0% для Операционного и Платежного клирингового центров и не менее 99,0% для Расчетного центра				

П2 = Т₁ – Т_{0'}

где:

Т₀, Т₁ – моменты возникновения события, приведшего к приостановлению оказания услуг платежной инфраструктуры;

Т_{0'}, Т_{1'} – моменты восстановления оказания услуг платежной инфраструктуры.

Показатель П2

расчитывается в часах/минутах/секундах.

Показатель П3

расчитывается по каждому ОУПИ

П3_{оп} = (N_{оп} / N^{общ}) × 100 % ,

П3_{нкп} = (N_{нкп} / N^{общ}) × 100 % ,

П3_{рп} = (N_{рп} / N^{общ}) × 100 % ,

№ п/п	Показатель БФПС	Пороговый уровень показателя БФПС	Категория Субъектов системы, влияющих на показатели БФПС	Порядок расчета показателя БФПС
			<p>$N_{\text{ак}} \quad N_{\text{рн}} \quad N_{\text{рн}}$ - количество распоряжений участников Страховой платежной системы, по которым в течение календарного месяца были оказаны услуги без нарушения регламента выполнения процедур;</p> <p>$N_{\text{общ}}^{\text{общ}} \quad N_{\text{ак}}^{\text{общ}} \quad N_{\text{рн}}^{\text{общ}}$ - общее количество распоряжений участников Страховой платежной системы, по которым в течение календарного месяца были оказаны услуги без нарушения регламента выполнения процедур.</p> <p>Показатель П3 рассчитывается ежемесячно в процентах с точностью до двух знаков после запятой (с округлением по математическому методу).</p> <p>Значение показателя П3 по Страховой платежной системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем ОУПИ в отношении всех видов оказываемых ими услуг.</p> <p>Показатель П4 рассчитывается как среднее значение коэффициента доступности Операционного центра за календарный месяц, рассчитываемое по следующей формуле:</p> $\text{П4} = \left(\sum_{i=1}^{M} \left(1 - \frac{D_i}{T_i} \right) / M \right) \times 100 \%,$ <p>где:</p>	
4.	Показатель доступности операционного центра платежной системы П4	Не менее - 96,0%	Операционный центр	

№ п/п	Показатель БФПС	Пороговый уровень показателя БФПС	Категория Субъектов системы, влияющих на показатели БФПС	Порядок расчета показателя БФПС
				<p>M - количество рабочих дней Страховой платежной системы в месяце,</p> <p>D_i - общая продолжительность всех приостановлений оказания операционных услуг Операционным центром за i-й рабочий день месяца в минутах,</p> <p>T_i - общая продолжительность времени оказания операционных услуг в течение i-го рабочего дня в минутах, установленная в соответствии с временным регламентом функционирования Страховой платежной системы.</p> <p>Показатель П4 рассчитывается ежемесячно в процентах с точностью до двух знаков после запятой (с округлением по математическому методу).</p>
5	Показатель изменился частоты Инцидентов П5	Не более 10,0%	Операционный центр, Платежный клиринговый центр, Расчетный центр Платежной системы (расчитывается по каждому ОУПИ и по Платежной системе в целом)	<p>Показатель П5 должен рассчитываться по Страховой платежной системе в целом и для каждого ОУПИ 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:</p>

№ п/п	Показатель БФПС	Пороговый уровень показателя БФПС	Категория Субъектов системы, влияющих на показатели БФПС	Порядок расчета показателя БФПС
				$\Pi 5 = \left(\frac{\sum_{i=1}^M KI_i / M}{\sum_{i=1}^N KI_i / N} - 1 \right) \times 100\%$ <p>где:</p> <p>KI_i - количество Инцидентов в течение i-го рабочего дня Страховой платежной системы оцениваемого календарного месяца,</p> <p>M - количество рабочих дней Страховой платежной системы в оцениваемом календарном месяце,</p> <p>N - количество рабочих дней Страховой платежной системы за 12 предыдущих календарных месяцев, включая оцениваемый месяц.</p> <p>Показатель П5 должен рассчитываться 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 0.</p>

4.2. Оценка влияния Инцидентов на БФПС:

Инцидент, влияющий на БФПС	Инцидент, не влияющий на БФПС
нарушен регламент выполнения процедур при одновременном нарушении порогового уровня показателя П2	не нарушен пороговый уровень показателя П4, рассчитанного по данным Инцидентам, и одновременно нарушен пороговый уровень показателя П3 и (или) показателя П5, рассчитанных по этим же Инцидентам
нарушен пороговый уровень показателя П1	
превышена продолжительность установленного Оператором Системы времени, в течение которого должно быть восстановлено оказание услуг платежной инфраструктуры, соответствующее требованиям к оказанию услуг	
одновременно нарушены пороговые уровни всех показателей П3, П4, П5, рассчитанных по данным Инцидентам, данные Инциденты признаются влияющими на БФПС	

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

Оператор Системы проводит оценку влияния на БФПС всех Инцидентов, произошедших в Страховой платежной системе в течение календарного месяца. Оценка влияния на БФПС данных Инцидентов проводится в течение 5 (пяти) рабочих дней после дня окончания календарного месяца, в котором возникли Инциденты.

В случае выявления Инцидентов или дополнительных обстоятельств Инцидентов, произошедших в Страховой платежной системе в течение календарного месяца, за который уже проведена оценка их влияния на БФПС, Оператор Системы должен проводить повторную оценку влияния на БФПС этих Инцидентов с учетом вновь выявленных обстоятельств в течение 5 (пяти) рабочих дней после дня окончания календарного месяца, в котором выявлены Инциденты или дополнительные обстоятельства.

Оператор Системы анализирует динамику фактических значений показателей БФПС, отклонения от пороговых значений, в том числе в целях

использования результатов анализа при оценке системы управления рисками и при оценке влияния Инцидентов на БФПС.

4.3. Сбор и обработка сведений по Страховой платежной системе, используемых для расчета показателей бесперебойности функционирования Страховой платежной системы.

Оператор Системы организует сбор и обработку от ОУПИ сведений по Страховой платежной системе, используемых для расчета показателей БФПС, а также сведения о произошедших в Страховой платежной системе Инцидентах на постоянной основе.

Сведения обо всех фактах возникновения/решения Инцидентов, связанных с нарушением БФПС, предоставляются ОУПИ по форме Приложение № 1 к Положению в кратчайшие сроки с момента возникновения (выявления) Инцидента путем направления его заполненной сканированной копии по электронной почте по адресу: ins-ps@ins-ps.ru, либо предоставляются ОУПИ по запросу Оператора Системы.

В целях обеспечения защиты информации в Страховой платежной системе и в рамках информационного взаимодействия с Оператором Системы ОПДС и ОУПИ предоставляют сведения обо всех выявленных в течение календарного месяца Инцидентах ИБ в соответствии с пунктом 6.2.10 Правил Страховой платежной системы.

В случае непредставления Субъектами системы указанной информации Оператор Системы считает, что Инциденты (Инциденты ИБ) не были выявлены.

Сведения об Инцидентах (Инцидентах ИБ) в Страховой платежной системе подлежат хранению не менее 5 (пяти) лет с даты получения указанных сведений от ОУПИ.

4.4. Контроль соблюдения процедур в Страховой платежной системе и оценка влияния Инцидентов на БФПС.

ОУПИ обязаны оперативно информировать Оператора Системы любым доступным способом о дате и времени проведения плановых и/или регламентных технологических работ в Страховой платежной системе.

Не позднее окончания рабочего дня, следующего за днем возникновения (выявления) произошедшего в Страховой платежной системе Инцидента, Оператор Системы проводит оценку влияния данного Инцидента на БФПС Страховой платежной системы, а также не позднее окончания рабочего дня, следующего за днем устранения последствий такого Инцидента (восстановления оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг).

Степень влияния Инцидента на БФПС Страховой платежной системы оценивается, в том числе на основе показателей БФПС, определенных в пункте 4.2 Положения.

Оператор Системы при выявлении нарушения порядка обеспечения БФПС Участниками и ОУПИ должен:

- информировать Участников и ОУПИ о выявленных в их деятельности нарушениях и устанавливать сроки устранения нарушений;
- осуществлять проверку результатов устранения нарушений и информировать Участников и ОУПИ, в деятельности которых выявлены нарушения, о результатах проведенной проверки.

Оператор Системы проводит анализ эффективности мероприятий по восстановлению оказания услуг платежной инфраструктуры, соответствующего требованиям к оказанию услуг, и использует полученные результаты при управлении рисками в Страховой платежной системе.

4.5. Уровни бесперебойности оказания услуг платежной инфраструктуры в Страховой платежной системе.

Оператор Системы использует в своей работе следующие уровни оказания услуг платежной инфраструктуры:

Нормальный – бесперебойное функционирование операционных и технологических средств платежной инфраструктуры, при котором ни один из показателей времени выполнения Бизнес-процессов не превышает установленных пороговых значений для нормального уровня функционирования (в пределах регламентов выполнения процедур).

Для Операционного центра указанный уровень оказания услуг платежной инфраструктуры определяется как время обработки информации, полученной от Участника-Страховщика в соответствии с пунктами 2, 3, 4, 5, 6 Приложения № 4 к Правилам Страховой платежной системы, которое не должно по времени превышать 30 (тридцать) минут.

Для Платежного клирингового центра и Расчетного центра указанный уровень оказания услуг платежной инфраструктуры определяется как время отклонения от временного регламента взаимодействия между Расчетным центром и Платежным клиринговым центром, которое не должно по времени превышать 30 (тридцать) минут (в связи с ситуацией или действиями, возникшими на стороне Платежного клирингового центра или Расчетного центра).

Допустимый – функционирование операционных и технологических средств платежной инфраструктуры с незначительными нарушениями регламентов выполнения процедур ОУПИ, при которых значения показателей времени выполнения Бизнес-процессов находятся в пределах, установленных для допустимого функционирования, то есть функционирование осуществляется с сохранением приемлемого качества предоставляемых услуг.

Для Операционного центра указанный уровень оказания услуг платежной инфраструктуры определяется как время обработки информации, полученной от Участника-Страховщика в соответствии с пунктами 2, 3, 4, 5, 6 Приложения № 4 к Правилам Страховой платежной системы, которое не должно по времени превышать 180 (сто восемьдесят) минут.

Для Платежного клирингового центра и Расчетного центра указанный уровень оказания услуг платежной инфраструктуры определяется как время отклонения от временного регламента взаимодействия между Расчетным центром и Платежным клиринговым центром, которое не должно по времени превышать 360 (триста шестьдесят) минут, в том числе при продлении Расчетной сессии на 1 (один) рабочий день (в связи с ситуацией или действиями, возникшими на стороне Платежного клирингового центра или Расчетного центра).

Критический – функционирование операционных и технологических средств платежной инфраструктуры с нарушением бесперебойности функционирования Системы, в том числе в чрезвычайных ситуациях, включая невозможность оказания услуг ОУПИ.

Для Операционного центра указанный уровень оказания услуг платежной инфраструктуры определяется как время обработки информации, полученной от Участника-Страховщика в соответствии с пунктами 2, 3, 4, 5, 6 Приложения № 4 к Правилам Страховой платежной системы, которое не должно превышать 540 (пятьсот сорок) минут.

Для Платежного клирингового центра и Расчетного центра указанный уровень оказания услуг платежной инфраструктуры признается критическим при значительном нарушении регламентов выполнения процедур.

Оператор Системы осуществляет оценку уровней оказания услуг платежной инфраструктуры, характеризующих качество функционирования операционных и технологических средств платежной инфраструктуры, на основании значений показателей оказания услуг Операционного центра, Платежного клирингового центра и Расчетного центра.

Оказание услуг платежной инфраструктуры в случае приостановления их оказания должно быть восстановлено в течение 6 (шести) часов, оказание услуг платежной инфраструктуры, соответствующее требованиям к оказанию услуг, в случае нарушения указанных требований, должно быть восстановлено в течение 72 (семидесяти двух) часов.

4.6. Требования к плану ОНиВД.

Оператор Системы проводит мероприятия по разработке, пересмотру и проверке (тестированию) плана ОНиВД не реже 1 (одного) раза в 2 (два) года.

План ОНиВД Оператора Системы должен содержать мероприятия, направленные на управление непрерывностью функционирования Страховой платежной системы в случае возникновения Инцидентов, связанных с приостановлением оказания услуг платежной инфраструктуры или нарушением установленных уровней оказания услуг платежной инфраструктуры, в том числе:

- мероприятия по переходу на резервный комплекс программных и (или) технических средств, а также мероприятия, осуществляемые в случае неработоспособности систем и сервисов Поставщиков услуг, нарушение предоставления которых способно привести к приостановлению оказания услуг платежной инфраструктуры;
- мероприятия по привлечению другого Расчетного центра и по переходу Участников-Страховщиков и Партнеров на обслуживание к вновь привлеченному Расчетному центру в течение срока, установленного Правилами Страховой платежной системы, в случаях:
 - превышения Расчетным центром времени восстановления оказания расчетных услуг при приостановлении их оказания более 2 (двух) раз в течение 3 (трех) месяцев подряд;
 - нарушения Правил Страховой платежной системы, выразившегося в отказе Расчетного центра в одностороннем порядке от оказания услуг Участнику-Страховщику (Участникам-Страховщикам) и/или Партнеру (Партнерам), не связанного с приостановлением (прекращением) участия в Страховой платежной системе в случаях, предусмотренных Правилами Страховой платежной системы.

4.7. Состав показателей уровня риска информационной безопасности в Страховой платежной системе:

Оператор Системы определяет требования к управлению риском информационной безопасности как одним из видов операционного риска и устанавливает показатели уровня риска информационной безопасности в Страховой платежной системе.

С целью регулирования процессов применения ограничений по параметрам операций по осуществлению переводов денежных средств в случае выявления факта превышения значений показателей уровня риска информационной безопасности в Страховой платежной системе в отношении ОПДС и ОУПИ Оператор Системы устанавливает следующие показатели:

Субъекты системы	Допустимые уровни риска информационной безопасности в Страховой платежной системе (в количественном показателе)*	Ограничения по параметрам операций по осуществлению переводов денежных средств в случае выявления факта превышения значений показателей уровня риска информационной безопасности
Операторы по переводу денежных средств	Низкий – 2 и менее Инцидентов ИБ в месяц; Средний – от 3-х до 4-х Инцидентов ИБ в месяц; Высокий – 5 и более Инцидентов ИБ в месяц.	Оператором Системы могут быть наложены ограничения на сумму единичной операции по переводу денежных средств. Оператором Системы могут быть наложены ограничения на временной период совершения операций.
Операторы услуг платежной инфраструктуры	Низкий – 2 и менее Инцидента ИБ в месяц; Средний – от 3-х до 4-х Инцидентов ИБ в месяц; Высокий – 5 и более Инцидентов ИБ в месяц.	Оператором Системы могут быть наложены ограничения на временной период совершения операций.

*В случаях, когда Инцидент ИБ повлек за собой последствия, вызвавшие наступление иных рисков высокого уровня, Оператор Системы вправе применить ограничения по параметрам операций по осуществлению переводов денежных средств в отношении ОПДС или ОУПИ, соответствующие ограничениям при уровне высокого риска информационной безопасности.

Условия снятия ограничений для ОПДС и ОУПИ по параметрам операций по осуществлению переводов денежных средств в случае выявления факта превышения значений показателей допустимого уровня риска информационной безопасности:

- в случае предоставления информации по устранению факторов, повлекших возникновение риска информационной безопасности, а также подробного описания принятых мер в целях минимизации возникновения риска информационной безопасности;
- в случае полного отсутствия рисков информационной безопасности в течение 3 (трех) месяцев, следующих за периодом, в рамках которого выявлено нарушение допустимого уровня рисков информационной безопасности.

5. ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ВЗАИМОДЕЙСТВИЯ СУБЪЕКТОВ СИСТЕМЫ ПО ОБЕСПЕЧЕНИЮ БФПС С УЧЕТОМ ОРГАНИЗАЦИОННОЙ МОДЕЛИ УПРАВЛЕНИЯ РИСКАМИ

5.1. Разграничение ответственности и полномочий между Субъектами системы по осуществлению управления рисками нарушения БФПС, в том числе обязанности Оператора Системы.

В обязанности Оператора Системы входит:

- осуществление координации деятельности Участников и ОУПИ по обеспечению БФПС;
- осуществление контроля соблюдения Участниками и ОУПИ порядка обеспечения БФПС путем постоянного мониторинга Значимых рисков;
- обеспечение возможности для Участников осуществить переход в течение срока, установленного Правилами Страховой платежной системы, на обслуживание к другому Расчетному центру в случае нарушения обслуживающим их Расчетным центром требований к бесперебойности оказания услуг платежной инфраструктуры, в том числе приостановления (прекращения) оказания услуг в порядке, установленном планом ОНиВД.

Участники организуют деятельность по реализации порядка обеспечения БФПС в рамках внутренних систем управления рисками своей деятельности.

В обязанности Участников входит:

- осуществление управления рисками нарушения БФПС в отношении их самих в соответствии с их внутренними документами;
- своевременное информирование Оператора Системы в случае увеличения рисков нарушения БФПС о приостановлении оказания услуг и о нарушении оказания услуг, предоставляемых в рамках Страховой платежной системы, и событиях, вызвавших операционные сбои, а также о событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, об их причинах и последствиях в соответствии с пунктом 4.11 Правил Страховой платежной системы (в случае непредоставления Участниками

указанной информации Оператор Системы считает, что риски нарушения БФПС не увеличивались);

- в случае выявления Оператором Системы фактов, свидетельствующих об увеличении рисков нарушения БФПС Участниками, предоставление разъяснения и принятие мер, направленных на снижение уровня выявленных рисков.

Обязанности ОУПИ по обеспечению бесперебойности оказания услуг платежной инфраструктуры, предоставляемых ими Участникам:

- осуществлять свою деятельность в соответствии с требованиями действующего законодательства Российской Федерации, нормативных актов Банка России и Правил Страховой платежной системы;
- при реализации внутренних систем управления рисками учитывать требования нормативных актов Банка России и Правил Страховой платежной системы;
- доводить до Оператора Системы информацию о возникновении нарушений оказания услуг, соответствующих требованиям к оказанию услуг, при которых превышено время восстановления оказания услуг платежной инфраструктуры в случае их приостановления и (или) время восстановления оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг, в случае их нарушения, возможных рисках для функционирования Страховой платежной системы, о принятии оперативных мер по устранению возникших нарушений и неисправностей в соответствии с пунктом 4.3 Положения;
- обеспечивать при оказании услуг уровень риска не выше приемлемого (допустимого);
- обеспечивать информационное взаимодействие между Субъектами системы в целях управления рисками нарушения БФПС;
- совершенствовать операционные и технологические средства и процедуры, информационные системы в целях снижения рисков нарушения БФПС.

ОПДС и ОУПИ также обязаны:

- соблюдать показатели уровня риска информационной безопасности в Страховой платежной системе, при которых уровень риска информационной

безопасности не превышает допустимые значения, установленные в пункте 4.7 Положения;

– предоставлять информацию Оператору Системы в рамках информационного взаимодействия об Инцидентах ИБ в соответствии с пунктом 6.2.10 Правил Страховой платежной системы.

5.2. Порядок информирования о событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев.

В случае возникновения спорных, чрезвычайных ситуаций или обстоятельств непреодолимой силы, влияющих на исполнение Субъектами системы своих обязательств в рамках взаимодействия в Страховой платежной системе, Субъекты системы, подвергшиеся влиянию указанных событий, незамедлительно предпринимают все зависящие от них действия, направленные на снижение негативных последствий, и действуют в рамках пунктов 4.10, 4.11 Правил Страховой платежной системы.

Оператор Системы информирует Банк России и Участников о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в соответствии с требованиями Указания Банка России № 3280-У.

При этом Оператор Системы информирует Участников-Страховщиков о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры, возникающих при осуществлении того вида переводов денежных средств, в рамках которого они присоединились к Правилам Страховой платежной системы.

Участников-Банков и Расчетный центр Оператор Системы информирует о случаях и причинах приостановления (прекращения) оказания услуг платежного клиринга.

Не является односторонним приостановлением (прекращением) оказания услуг платежной инфраструктуры Участникам, осуществляемое в соответствии с Правилами Страховой платежной системы в целях осуществления контроля за соблюдением Правил Страховой платежной системы Участниками и ОУПИ, обеспечения бесперебойности функционирования Страховой платежной системы.

6. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ОПЕРАТОРАМИ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ И УЧАСТНИКАМИ СТРАХОВОЙ ПЛАТЕЖНОЙ СИСТЕМЫ ПОРЯДКА ОБЕСПЕЧЕНИЯ БФПС

Оператор Системы осуществляет на постоянной основе контроль за соблюдением Участниками, ОУПИ порядка обеспечения БФПС посредством следующих мероприятий:

- осуществление контроля за соблюдением Правил Страховой платежной системы в соответствии с пунктом 3.2 Правил Страховой платежной системы;
- проведение дистанционного контроля и/или направления запросов Участникам, ОУПИ о предоставлении информации, необходимой Оператору Системы для осуществления контроля;
- предоставление Участниками, привлеченными на договорной основе ОУПИ, информации о своей деятельности Оператору Системы в соответствии с пунктом 4.12 Правил Страховой платежной системы;
- предоставления ОУПИ информации о Риск-событиях в соответствии с пунктом 4.3 Положения;
- предоставления Участниками и ОУПИ информации о приостановлении оказания услуг и о нарушении оказания услуг, оказываемых в рамках Страховой платежной системы, и событиях, вызвавших операционные сбои, а также о событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, об их причинах и последствиях в соответствии с пунктом 4.11 Правил Страховой платежной системы;
- предоставления Участниками и ОУПИ информации об Инцидентах ИБ в рамках информационного взаимодействия в соответствии с пунктом 6.2.10 Правил Страховой платежной системы;
- проведение переписки (в том числе по электронной почте) с Участниками, ОУПИ о результатах осуществления мониторинга и фиксирования информации, связанной с обеспечением БФПС, относящихся к деятельности соответствующего Участника, ОУПИ, в первую очередь - о доступном остатке денежных средств на счетах Участников. Оператором Системы для осуществления контроля за

соблюдением Участниками, ОУПИ порядка обеспечения БФПС могут реализовываться иные мероприятия.

Оператор Системы при выявлении нарушения порядка обеспечения БФПС Участниками и ОУПИ должен:

- информировать Участников и ОУПИ о выявленных в их деятельности нарушениях;
- устанавливать сроки устранения нарушений;
- осуществлять проверку результатов устранения нарушений;
- информировать операторов Участников и ОУПИ, в деятельности которых выявлены нарушения, о результатах проведенной проверки.

Субъекты системы несут ответственность за неисполнение порядка обеспечения БФПС в соответствии с законодательством Российской Федерации, Правилами Страховой платежной системы и договорами, заключенными в связи с участием в Страховой платежной системе.

Оператор Системы в случае выявления нарушений применяет меры воздействия к Участникам и ОУПИ в соответствии с Правилами Страховой платежной системы и действующими договорами.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

7.1. Положение вступает в силу со дня его утверждения Генеральным директором ООО «СПС» и действует без ограничения срока действия (до внесения соответствующих изменений, дополнений или принятия нового Положения).

7.2. Все вопросы, не урегулированные в Положении, регулируются действующим законодательством Российской Федерации, нормативными актами Банка России, Правилами Страховой платежной системы и иными внутренними документами ООО «СПС».

Приложение № 1
к Положению об организации управления рисками и обеспечения
бесперебойности функционирования Страховой платежной системы

Форма

Сведения обо всех фактах возникновения/решения Инцидентов, связанных с нарушением БФПС

« » 20 Г.

№ п/п	Время и дата возникновения Инцидента	Найменование одного или нескольких Бизнес-процессов, в ходе которых произошел Инцидент	Наличие (отсутствие) факта приостановления (прекращения) оказания УПИ в результате Инцидента	Степень влияния Инцидента на функционирование Платежной системы ²	Время и дата восстановления оказания услуг платежной инфраструктуры в случае пристановления их оказания	Мероприятия по устранению Инцидента	Планируемая продолжительность мероприятия по устранению Инцидента	Фактическая продолжительность мероприятия по устранению Инцидента	Дата восстановления оказания УПИ, соответствующего требованиям к оказанию УПИ	Неблагоприятные последствия Инцидента для Субъектов системы ³
1	2	3	4	5	6	7	8	9	10	11
									12	13
									14	

Наименование Субъекта системы _____

Должность уполномоченного лица _____
подпись _____ ФИО _____

М.П.

¹ влияние Инцидента на БФПС, определяемое с учетом того, что Оператор Системы должен проводить оценку влияния на БФПС каждого произошедшего в Страховой платежной системе Инцидента не позднее окончания рабочего дня, следующего за днем его возникновения (выявления), а также не позднее окончания рабочего дня, следующего за днем устранения Инцидента (восстановления оказания услуг платежной инфраструктуры, соответствующего требованием к оказанию услуг);

² степень влияния Инцидента на функционирование Страховой платежной системы в зависимости от количества ОУПИ, и (или) количества и значимости Участников, на которых оказал непосредственное влияние Инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных Распоряжений, и иных факторов;

³ неблагоприятные последствия Инцидента для Субъектов системы, в том числе:

- сумма денежных средств, уплаченных Оператором Системы и (или) взысканных с Оператора Системы;
- сумма денежных средств, уплаченных ОУПИ и (или) взысканных с ОУПИ;
- количество и сумма неисполненных и (или) несвоевременно исполненных, и (или) ошибочно исполненных Распоряжений, на исполнение которых оказал влияние Инцидент;
- продолжительность приостановления оказания услуг платежной инфраструктуры.

Приложение № 2
к Положению об организации управления рисками и обеспечения
бесперебойности функционирования Страховой платежной системы

Профили рисков

№ п/п	Профили рисков	Описан- ие Риск- события	Описани- (источник) возникнове- ния Риск- события	Описан- ие Бизнес- процесса	Субъект системы, являющийся владельцем Бизнес- процесса	Вероят- ность наступле- ния Риск- события	Описание последствий Риск- события	Оценка последствий Риск- события	Описание Бизнес- процессов, на которые влияет Риск- событие	Субъекты системы, на которые влияет Риск- событие	Уровень применения способов управления рисками в Страховой платежной системе	Уровень допустимого риска	Перечень способов управления рисками	Уровень остаточного риска после применения способов управления рисками в Страховой платежной системе
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	Профиль операционного риска	1.1						1.1.1						
			1.п ¹					1.1.м ¹						
2	Профиль правового риска	2.1							1.п.1					
			2.п ²						1.п.м					
3	Профиль кредитного риска								2.1.1					
									2.1.м ¹					
4	Профиль риска ликвидности								2.п.1					
									2.п.м					
5	Профиль общего коммерческого риска													
6	Профиль системного риска													

¹ - м - количество последствий для каждого из выявленных Риск-событий;

² - п - количество Риск-событий для каждого из рисков в Страховой платежной системе;

Приложение № 3

к Положению об организации управления рисками и обеспечения бесперебойности функционирования Страховой платежной системы

**Перечень критически важных Бизнес-процессов в
Страховой платежной системе**

Бизнес-процесс	Процедуры	Оператор услуг платежной инфраструктуры, реализующий Бизнес-процесс
Оказание операционных услуг	Обеспечение обмена информацией между Участниками-Страховщиками, состав которой определен пунктами 2-6 Приложения № 4 к Правилам Страховой платежной системы, обеспечение обмена электронными информационными сообщениями между Платежным клиринговым центром и Расчетным центром	Операционный центр
	Формирование и удостоверение Распоряжений на основании информации, полученной от Участников-Страховщиков в рамках информационного взаимодействия, состав которой определен пунктами 2-6 Приложения № 4 к Правилам Страховой платежной системы, для осуществления перевода денежных средств, предусмотренных Разделом 2 Правил Страховой платежной системы, и их передачу в Платежный клиринговый центр	
	Обеспечение защиты информации при осуществлении переводов денежных средств	
Оказание услуг платежного клиринга	Обеспечение проведения платежного клиринга в Страховой платежной системе в соответствии с порядком, установленным Правилами Страховой платежной системы	Платежный клиринговый центр
	Обеспечение защиты информации при осуществлении переводов денежных средств	
Оказание расчетных услуг	Обеспечение проведения расчетов в Страховой платежной системе согласно порядку, определенному Правилами Страховой платежной системы	Расчетный центр

Обеспечение защиты информации при
осуществлении переводов денежных средств

Приложение № 4
к Положению об организации управления рисками и обеспечения
бесперебойности функционирования Страховой платежной системы

Методика анализа рисков

1. Методика анализа рисков в Страховой платежной системе предусматривает выполнение следующих мероприятий:

- формирование и поддержание в актуальном состоянии перечней Бизнес-процессов (Приложение № 3 к Положению);
- разработку и поддержание в актуальном состоянии классификаторов (структурированных перечней) рисков в Страховой платежной системе, Риск-событий, причин Риск-событий (пункт 3.6 Положения и Таблица 1 Приложения № 4 к Положению);
- проведение анализа Бизнес-процессов в Страховой платежной системе, в том числе анализа программных и (или) технических средств ОУПИ, учитывая факт привлечения ими поставщиков услуг, и других факторов, влияющих на БФПС;
- формирование перечня возможных Риск-событий для каждого Бизнес-процесса с указанием причин Риск-событий и их последствий (Приложение № 5 к Положению);
- определение для каждого из выявленных рисков в Страховой платежной системе Уровня присущего риска до применения способов управления рисками в Страховой платежной системе и установление Уровня допустимого риска (Таблица 1 Приложения № 4 к Положению);
- сопоставление Уровня присущего риска до применения способов управления рисками в Страховой платежной системе и Уровня допустимого риска по каждому из выявленных рисков в Страховой платежной системе для определения Значимых рисков (Таблица 2 Приложения № 4 к Положению);
- применение способов управления рисками в Страховой платежной системе для каждого из Значимых рисков (пункт 5.3 Правил Страховой платежной системы) и последующее определение для них Уровня остаточного риска

после применения способов управления рисками в Страховой платежной системе;

- сопоставление Уровня остаточного риска после применения способов управления рисками в Страховой платежной системе и Уровня допустимого риска для каждого из Значимых рисков и принятие решения о необходимости применения других способов управления рисками в Страховой платежной системе в дополнение к ранее примененным способам;
- мониторинг рисков в Страховой платежной системе, в том числе Уровня остаточного риска после применения способов управления рисками в Страховой платежной системе, его соответствия Уровню допустимого риска;
- составление и пересмотр (актуализацию) профиля каждого из Значимых рисков, включая профиль риска нарушения БФПС.

2. Оператор Системы в целях управления рисками в Страховой платежной системе разрабатывает методику анализа рисков в Страховой платежной системе, включая риск нарушения БФПС. Разработанная Оператором Системы методика анализа рисков использует метод индексов риска, определенный в Стандарте, метод экспертных оценок, а также применение элементов методик, основанных на статистическом анализе функционирования Страховой платежной системы.

Методика анализа рисков в Страховой платежной системе согласно Положению Банка России № 607-П и пункту 5.2.4.2 Правил Страховой платежной системы обеспечивает:

- выполнение процедур выявления Оператором Системы рисков в Страховой платежной системе не реже 1 (одного) раза в год;
- проведение анализа рисков в Страховой платежной системе;
- выявление Риск-событий 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 Страховой платежной системе Уровня присущего риска до применения способов управления рисками в Страховой платежной системе, а также Уровня допустимого риска;
- определение Значимых рисков;

- определение для каждого из Значимых рисков Уровня остаточного риска после применения способов управления рисками в Страховой платежной системе.

3. Выявление и анализ рисков в Страховой платежной системе проводится Оператором Системы с применением следующих элементов методик, основанных на статистическом анализе функционирования системы:

- анализ, отслеживание и фиксирование параметров работы Участников и ОУПИ в Страховой платежной системе, в том числе соблюдение порядка расчетов согласно раздела 7 Правил Страховой платежной системы;
- накопление и статистический анализ информации о нестандартных, спорных и чрезвычайных ситуациях, а также иных событий реализации рисков системы.

Для определения уровня рисков Оператор Системы использует понятия «Вероятность реализации риска» и «Возможные неблагоприятные последствия» (размер возможных потерь или степень влияния на БФПС) и методом экспертных оценок определяет для каждого выявленного Риск-события их по шкале от 1 до 0, где соответственно:

- «0» – маловероятная и минимальная;
- «1» – наиболее возможная и максимальная.

Для оценки Уровней присущих рисков Оператор Системы рассчитывает индексы рисков как средние значения по формуле:

$$И = (B + П) / 2, \text{ где}$$

- И – индекс риска;
- В – вероятность реализации риска;
- П – возможные неблагоприятные последствия.

Уровни присущих рисков определяем в зависимости от значений индексов рисков:

- индекс риска 0.8 и более – Уровень присущего риска высокий (критический);
- индекс риска больше 0.4, но меньше 0.8 – Уровень присущего риска средний;
- индекс риска 0.4 и менее – Уровень присущего риска низкий.

Низкий уровень риска - уровень риска, в результате которого потенциальные/понесенные убытки не оказывают влияние на БФПС;

Средний уровень риска - уровень риска, в результате которого потенциальные/понесенные убытки оказывают влияние на БФПС допустимого характера;

Высокий уровень риска - уровень риска, в результате которого потенциальные/понесенные убытки оказывают критическое влияние на БФПС.

В Страховой платежной системе устанавливаются уровни допустимых рисков при значении индексов риска менее 0.8 по каждому виду рисков.

Уровни допустимых рисков определяются в зависимости от уровня присущего риска, индексов риска и количества выявленных Риск-событий:

- при выявлении единичного Риск-события по каждому виду рисков - низкий и средний уровни присущего риска;

- при выявлении нескольких Риск-событий по каждому виду рисков сумма индексов рисков не должны превышать 0.8. В случае превышения указанного значения Уровень присущего риска принимается за высокий (критический).

При определении уровня присущего риска, кроме данных, определяемых в настоящем пункте Приложения, используется информация, указанная в пункте 3.6 Положения (перечень рисков), в пунктах 3.6.1 – 3.6.6 Положения (причины возникновения и/или источники Риск-событий, общие принципы управления рисками, включающие меры для достижения и минимизации допустимого уровня риска и предотвращения рисков), Приложении № 3 к Положению (Субъекты системы, Бизнес-процессам, которым присущи данные Риск-события).

Таблица 1

**Классификатор (структурированный перечень) рисков, Риск-событий,
причин Риск-событий**

Перечень рисков	Риск-события	Причины возникновения и/или источники Риск-событий	Меры по достижению и поддержанию Уровня допустимого риска	Субъекты системы, Бизнес-процессам которых присущи данные Риск-события	Вероятность реализации риска (В)	Возможные неблагоприятные последствия (П)	Индекс риска (И)	Уровень присущего риска
Правовой риск	Нарушение Субъектами системы требований действующего законодательства Российской Федерации, нормативных актов Банка России	Несоблюдение Субъектами системы требований действующего законодательства Российской Федерации. Наличие правовых коллизий и (или) правовой неопределенности в законодательстве РФ, нормативных актах Банка России	Применение принципов управления рисками, указанных в пункте 3.6.1 Положения	Оператор Системы, ОУПИ, Участники-Банки, Участники-Страховщики	0.1	0.5	0.3	Низкий
	Нарушение Субъектами системы Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и документов Операторов услуг платежной инфраструктуры	Несоблюдение Субъектами системы требований Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и Операторов услуг платежной инфраструктуры	Применение принципов управления рисками, указанных в пункте 3.6.1 Положения	Оператор Системы, ОУПИ, Участники-Банки, Участники-Страховщики	0.4	0.5	0.5	Средний
Операционный риск	Отказы и аварии в работе информационных и технологических систем	Несоразмерность (недостаточность) функциональных возможностей (характеристик) применяемых в Страховой платежной системе информационных, технологических и других систем и (или) их отказов (нарушений функционирования)	Применение принципов управления рисками, указанных в пункте 3.6.2 Положения	Оператор Системы, ОУПИ, Участники-Банки, Участники-Страховщики	0.6	0.8	0.7	Средний
	Недостатки в организации и выполнении технологических и управленческих процессов	Несоответствие характера и масштаба деятельности Страховой платежной системы требованиям действующего законодательства Российской Федерации,	Применение принципов управления рисками, указанных в пункте 3.6.2 Положения	Оператор Системы, ОУПИ, Участники-Банки, Участники-Страховщики	0.3	0.6	0.5	Средний

		Правилам Страховой платежной системы, внутренним регламентам Оператора Системы						
	Ошибочные или противоправные действия работников Субъектов системы	Нарушение работниками требований действующего законодательства Российской Федерации, Правил Страховой платежной системы, внутренних регламентов Оператора Системы	Применение принципов управления рисками, указанных в пункте 3.6.2 Положения	Оператор Системы, ОУПИ, Участники-Банки, Участники-Страховщики	0.4	0.8	0.6	Средний
	События, причины возникновения которых не связаны с деятельностью Субъектов системы, включая ошибочные и противоправные действия третьих лиц и чрезвычайные ситуации	Внешнее воздействие, в т.ч. чрезвычайные ситуации	Применение принципов управления рисками, указанных в пункте 3.6.2 Положения. Соблюдение плана ОНиВД	Оператор Системы, ОУПИ, Участники-Банки, Участники-Страховщики	0.5	0.8	0.7	Средний
	Нарушение защиты информации	Распространяющийся в прогрессии вредоносный код и злонамеренные действия работников Субъектов системы и/или третьих лиц на различных уровнях, а именно: - на физическом уровне информационной инфраструктуры; - на уровне сетевого оборудования; - на уровне сетевых приложений и сервисов; - на уровне операционных систем	Применение принципов управления рисками, указанных в пункте 3.6.2 Положения	Оператор Системы, ОУПИ, Участники-Банки, Участники-Страховщики	0.6	0.8	0.7	Средний
	Ненадлежащее обеспечение защиты информации	Недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации, недостатки прикладного программного обеспечения автоматизированных систем и приложений, а также	Применение принципов управления рисками, указанных в пункте 3.6.2 Положения	Оператор Системы, ОУПИ, Участники-Банки	0.6	0.8	0.7	Средний

		несоблюдение требований к указанным процессам деятельности ОПДС и ОУПИ						
Кредитный риск	Невыполнение Участниками Системы договорных обязательств перед Расчётыным центром в установленный срок или в будущем	Из-за несоблюдения платежных и расчетных процессов не будут своевременно оплачены требования Участников-Страховщиков, возникающие у них по договорным обязательствам в результате проведения расчетов по итогам платежного клиринга	Применение принципов управления рисками, указанных в пункте 3.6.3 Положения	Расчетный центр, Участники-Банки, Участники-Страховщики	0.5	0.4	0.5	Средний
Риск ликвидности	Отсутствие у Участников Системы денежных средств, достаточных для своевременного выполнения принятых на себя финансовых обязательств перед другими Участниками Системы	Недостаточно денежных средств у Участника-Страховщика в Системе для своевременного выполнения принятых на себя финансовых обязательств перед другими Участниками Системы в полной мере	Применение принципов управления рисками, указанных в пункте 3.6.4 Положения	Участники-Банки, Участники-Страховщики	0.8	0.4	0.6	Средний
	Запрет расходных операций, арест денежных средств Участников-Страховщиков, находящихся на Счете Участника, на сумму превышающую сумму принятых на себя финансовых обязательств перед другими Участниками-Страховщиками	Применение ограничений прав на распоряжение частью или всей суммой денежных средств, находящихся на Счете Участника, открытом в Расчетном центре и предназначенном для своевременного выполнения принятых на себя финансовых обязательств перед другими Участниками-Страховщиками в полной мере	Применение принципов управления рисками, указанных в пункте 3.6.4 Положения	Расчетный центр, Участники-Страховщики	0.8	0.4	0.6	Средний

Общий коммерческий риск	Ухудшение финансового состояния Оператора Системы и\или ОУПИ, не связанного с реализацией кредитного риска и риска ликвидности Страховой платежной системы	Потеря деловой репутации	Использование современных технологий. Поддержание положительной деловой репутации Страховой платежной системы в СМИ	Оператор Системы, ОУПИ, Участники-Банки, Участники-Страховщики	0.2	0.3	0.3	Низкий
Системный риск	Неспособность одного или нескольких Субъектов системы исполнить принятые на себя обязательства или нарушений в самой Страховой платежной системе, которое вызовет неспособность большинства или всех Субъектов системы исполнить свои обязательства в срок	Распространение между Субъектами системы последствий основных рисков, указанных в пунктах. 3.6.1 - 3.6.5 Положения, вызывающих нарушения функционирования Страховой платежной системы	Применение принципов управления рисками, указанных в пункте 3.6.6 Положения	Оператор Системы	0.2	0.3	0.3	Низкий

После определения Уровня присущего риска Оператор Системы проводит сравнение Уровня присущего риска с Уровнем допустимого риска (Таблица 2 Приложения № 4 к Положению).

Оператор Системы, используя способы управления рисками (пункт 5.3 Правил Страховой платежной системы), в целях минимизации Уровней присущих рисков по Значимым рискам, предотвращения и минимизации Риск-событий, их причин и последствий, оценивает Уровень остаточного риска аналогично Уровню присущего риска. Если при применении способов управления рисками устранены источники и причины выявленных Риск-событий, Уровень остаточного риска считается равным 0.

4. Профили рисков (Приложение № 2 к Положению) должны составляться по всем Значимым рискам в Страховой платежной системе, используя данные из Таблицы 1 Приложения № 4 к Положению. Профиль риска нарушения БФПС должен составляться как сводный профиль в отношении всех Значимых рисков в Страховой платежной системе.

Таблица 2

Сравнение уровня присущего риска с уровнем допустимого риска

Наименование	Уровень присущего риска	Уровень допустимого риска
Правовой риск в Бизнес-процессах Субъекта системы	не выявлен/низкий/средний	не превышен
	Высокий	превышен
Операционный риск в Бизнес-процессах Субъекта системы	не выявлен/низкий/средний	не превышен
	Высокий	превышен
Кредитный риск в Бизнес-процессах Субъекта системы	не выявлен/низкий/средний	не превышен
	Высокий	превышен
Риск ликвидности в Бизнес-процессах Субъекта системы	не выявлен/низкий/средний	не превышен
	Высокий	превышен
Общий коммерческий риск в Бизнес-процессах Субъекта системы	не выявлен/низкий/средний	не превышен
	Высокий	превышен
Системный риск в Бизнес-процессах Субъекта системы	не выявлен/низкий/средний	не превышен
	Высокий	превышен
П1, П2, П3, П4, П5 для ОУПИ	в пределах порогового уровня	не превышен
	пороговый уровень превышен	превышен

Для Оператора Системы анализируются правовой, операционный, общий коммерческий и системный риски. Для снижения системного риска Оператор Системы организует систему управления рисками, направленную на снижение основных видов рисков.

Для Операционного центра: правовой, операционный, общий коммерческий риски и показатели П1 – П5.

Для Платежного клирингового центра: правовой, операционный, общий коммерческий риски и показатели П1 – П3, П5.

Для Расчетного центра: правовой, операционный, кредитный, ликвидности и общий коммерческий риски и показатели П1 – П3, П5.

Для Участника: правовой, операционный, кредитный, ликвидности и общий коммерческий риски.

5. Оценка системы управления рисками:

Таблица 3

№ п/п	Параметры оценки	Вес	Балл*	Значение**
1	Непрерывность определения уровней рисков	2	1	
2	Непрерывность определения показателей	2	1	
3	Оперативное внесение изменений в управление рисками в случае изменения внешних и внутренних факторов	1	1	
4	Снижение остаточных уровней риска в случае выявления значимых рисков	3	1	
5	Соблюдение системы полномочий и принятия решений	3	1	
6	Поддержание информационной системы в актуальном состоянии	1	1	
7	Соблюдение показателей в пределах пороговых уровней	2	1	
8	Подготовка управленческой отчётности	2	1	
	Оценка (итого) ***			

* При оценке параметров рекомендуется следующее определение баллов:

Балл	Расшифровка значения
1	в течение года нарушения отсутствовали
2	в течение года выявлено не более 5 нарушений
3	в течение года выявлено более 5 нарушений

** Значение параметра оценки определяется путем умножения веса показателя на балл.

*** Итоговое значение оценки рассчитывается как сумма произведения веса на балл деленное на сумму весов указанных параметров оценки.

Оценку системы управления рисками определяем в зависимости от значения соответствующего показателя на основании шкалы, приведенной в Таблице 4.

Таблица 4
Шкала оценки системы управления рисками

Критерии оценки	Хорошая	Удовлетворительная	Неудовлетворительная
Значение показателя	< 1.5	≥ 1.5 и < 2.3	≥ 2.3

Приложение № 5

к Положению об организации управления рисками и обеспечения
бесперебойности функционирования Страховой платежной системы

**Перечень основных внутренних Риск-событий для каждого Бизнес-процесса
Страховой платежной системы, их причин и последствий**

Данный перечень не является исчерпывающим, возможно его дополнение или изменение при получении новой информации в процессе функционирования Страховой платежной системы

Бизнес-процессы	Риск	Риск-событие	Причины Риск-события	Последствия Риск-события
Оказание операционных услуг	Операционный риск	Отказы и аварии в работе информационных и технологических систем	Несоразмерность (недостаточность) функциональных возможностей (характеристик) применяемых в Страховой платежной системе информационных, технологических и других систем и (или) их отказов (нарушений функционирования)	Приостановление оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг. Нарушение оказания услуг платежной инфраструктуры
		Недостатки в организации и выполнении технологических и управленческих процессов	Несоответствие характера и масштаба деятельности Страховой платежной системе требованиям действующего законодательства Российской Федерации, Правилам Страховой платежной системы, внутренним регламентам Оператора Системы	
		Ошибочные или противоправные действия работников Субъектов системы	Нарушение работниками требований действующего законодательства Российской Федерации, Правил Страховой платежной системы, внутренних регламентов Оператора Системы	
		События, причины возникновения которых не связаны с деятельностью Субъектов системы, включая ошибочные и противоправные действия третьих лиц и чрезвычайные ситуации	Внешнее воздействие, в т.ч. чрезвычайные ситуации	
		Нарушение информационной безопасности	Распространяющийся в прогрессии вредоносный код и злонамеренные действия работников Субъектов системы и/или третьих лиц на различных уровнях, а именно: - на физическом уровне информационной инфраструктуры; - на уровне сетевого оборудования; - на уровне сетевых приложений и сервисов;	

			- на уровне операционных систем	
	Ненадлежащее обеспечение защиты информации		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 ОПДС и ОУПИ	
Правовой риск	Нарушение Субъектами системы требований действующего законодательства Российской Федерации, нормативных актов Банка России		Несоблюдение Субъектами системы требований действующего законодательства Российской Федерации. Наличие правовых коллизий и (или) правовой неопределенности в законодательстве РФ, нормативных актах Банка России	
	Нарушение Субъектами системы Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и документов ОУПИ		Несоблюдение Субъектами системы требований Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и ОУПИ	
Общий коммерческий риск	Ухудшение финансового состояния Операционного центра, не связанного с реализацией кредитного риска и риска ликвидности Страховой платежной системы		Потеря деловой репутации	
Оказание услуг платежного клиринга	Операционный риск	Отказы и аварии в работе информационных и технологических систем	Несоразмерность (недостаточность) функциональных возможностей (характеристик) применяемых в Страховой платежной системе информационных, технологических и других систем и (или) их отказов (нарушений функционирования)	Приостановление оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг. Нарушение оказания услуг платежной инфраструктуры
		Недостатки в организации и выполнении технологических и управленческих процессов	Несоответствие характера и масштаба деятельности Страховой платежной системы требованиям действующего законодательства Российской Федерации, Правилам Страховой платежной системы, внутренним регламентам Оператора Системы	
		Ошибочные или противоправные действия работников Субъектов системы	Нарушение работниками требований действующего законодательства Российской Федерации, Правил Страховой платежной системы, внутренних регламентов Оператора Системы	

		<p>События, причины, возникновения которых не связаны с деятельностью Субъектов системы, включая ошибочные и противоправные действия третьих лиц и чрезвычайные ситуации</p>	Внешнее воздействие, в т.ч. чрезвычайные ситуации	
		<p>Нарушение информационной безопасности</p>	<p>Распространяющийся в прогрессии вредоносный и злонамеренные действия персонала Субъектов системы и/или третьих лиц на различных уровнях, а именно:</p> <ul style="list-style-type: none"> - на физическом уровне информационной инфраструктуры; - на уровне сетевого оборудования; - на уровне сетевых приложений и сервисов; - на уровне операционных систем 	
		<p>Ненадлежащее обеспечение защиты информации</p>	<p>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 ОПДС и ОУПИ</p>	
Правовой риск	<p>Нарушение Субъектами системы требований действующего законодательства Российской Федерации, нормативных актов Банка России</p>	<p>Несоблюдение Субъектами системы требований действующего законодательства Российской Федерации.</p> <p>Наличие правовых коллизий и (или) правовой неопределенности в законодательстве РФ, нормативных актах Банка России</p>		
	<p>Нарушение Субъектами системы Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и документов ОУПИ</p>	<p>Несоблюдение Субъектами системы требований Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и ОУПИ</p>		
Общий коммерческий риск	<p>Ухудшение финансового состояния Платежного клирингового центра, не связанного с реализацией кредитного риска и риска ликвидности Страховой платежной системы</p>	Pотеря деловой репутации		
Оказание расчетных услуг	Кредитный риск	<p>Невыполнение Участниками Системы договорных обязательств перед Расчетным центром в установленный срок или в будущем</p>	<p>Из-за несоблюдения платежных и расчетных процессов не будут своевременно оплачены требования Участников-Страховщиков, возникающие у них по договорным обязательствам в результате проведения расчетов по итогам платежного клиринга</p>	<p>Приостановление оказания услуг платежной инфраструктуры, соответствующих требованиям к оказанию услуг.</p> <p>Нарушение</p>

	Риск ликвидности	Отсутствие у Участников Системы денежных средств, достаточных для своевременного выполнения принятых на себя финансовых обязательств перед другими Участниками Системы	Недостаточно денежных средств у Участника-Страховщика в Системе для своевременного выполнения принятых на себя финансовых обязательств перед другими Участниками Системы в полной мере	оказания услуг платежной инфраструктуры
		Запрет расходных операций, арест денежных средств Участников-Страховщиков, находящихся на Счете Участника, на сумму превышающую сумму принятых на себя финансовых обязательств перед другими Участниками-Страховщиками	Применение ограничений прав на распоряжение частью или всей суммой денежных средств, находящихся на Счете Участника, открытом в Расчетном центре и предназначенном для своевременного выполнения принятых на себя финансовых обязательств перед другими Участниками-Страховщиками в полной мере	
	Операционный риск	Отказы и аварии в работе информационных и технологических систем	Несоразмерность (недостаточность) функциональных возможностей (характеристик) применяемых в Страховой платежной системе информационных, технологических и других систем и (или) их отказов (нарушений функционирования)	
		Недостатки в организации и выполнении технологических и управленческих процессов	Несоответствие характера и масштаба деятельности Страховой платежной системе требованиям действующего законодательства Российской Федерации, Правилам Страховой платежной системы, внутренним регламентам Оператора Системы	
		Ошибочные или противоправные действия работников Субъектов системы	Нарушение работниками требований действующего законодательства Российской Федерации, Правил Страховой платежной системы, внутренних регламентов Оператора Системы	
		События, причины возникновения которых не связаны с деятельностью Субъектов системы, включая ошибочные и противоправные действия третьих лиц и чрезвычайные ситуации	Внешнее воздействие, в т.ч. чрезвычайные ситуации	
		Нарушение информационной безопасности	Распространяющийся в прогрессии вредоносный код и злонамеренные действия работников Субъектов системы и/или третьих лиц на различных уровнях, а именно: - на физическом уровне информационной инфраструктуры; - на уровне сетевого оборудования; - на уровне сетевых приложений и сервисов; - на уровне операционных систем	

		Ненадлежащее обеспечение защиты информации	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 ОПДС и ОУПИ	
Правовой риск		Нарушение Субъектами системы требований действующего законодательства Российской Федерации, нормативных актов Банка России	Несоблюдение Субъектами системы требований действующего законодательства Российской Федерации. Наличие правовых коллизий и (или) правовой неопределенности в законодательстве РФ, нормативных актах Банка России	
		Нарушение Субъектами системы Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и документов ОУПИ	Несоблюдение Субъектами системы требований Правил Страховой платежной системы, договоров, заключенных между Субъектами системы, документов Оператора Системы и ОУПИ	
	Общий коммерческий риск	Ухудшение финансового состояния Расчетного центра, не связанного с реализацией кредитного риска и риска ликвидности Страховой платежной системы	Потеря деловой репутации	