Утверждены Решением
Общего собрания участников
№1/ППС от 13.02.2026 г.

# ПРАВИЛА ПЛАТЕЖНОЙ СИСТЕМЫ
# “Система банковской кооперации”
Версия 3.5

г. Москва, 2026 г.

ОГЛАВЛЕНИЕ

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Платежная система.

Платежная система “Система банковской кооперации” (далее Система или Платежная Система) - совокупность организаций, взаимодействующих по Правилам Системы в целях осуществления перевода денежных средств, включающая оператора Системы, операторов услуг платежной инфраструктуры и участников. Система создана в Российской Федерации и действует в соответствии с требованиями Федерального закона № 161-ФЗ «О национальной платежной системе». За пределами Российской Федерации Платежная Система осуществляет свою деятельность с учетом требований законодательства стран осуществления деятельности.

Оператором Платежной системы (далее Оператором) является Общество с ограниченной ответственностью “Оператор банковской кооперации” (ООО “Оператор банковской кооперации”).

Целью создания Системы является оказание услуг по переводу денежных средств, в том числе трансграничных, посредством кооперации российских и иностранных банков (и иных организаций, приравненных регуляторами к банкам по возможности оказания платежных услуг), совместно использующих платежную инфраструктуру Системы.

1.2. Правила платежной системы.

Настоящие Правила Платежной Системы (далее «Правила»), включая все Приложения, составлены Оператором в соответствии с положениями законодательства Российской Федерации, а также политиками и процедурами Системы и представляют собой документ, устанавливающий условия участия в Платежной Системе, условия осуществления перевода денежных средств в рамках Платежной Системы, порядок оказания услуг платежной инфраструктуры, а также иные условия, определенные настоящими Правилами. Для целей настоящих Правил под законодательством Российской Федерации (Законодательством) понимаются все законы и нормативные акты, действующие в Российской Федерации, в том числе нормативные акты Банка России.

Правила, включая тарифы, являются публично доступными и размещаются на официальном сайте Оператора за исключением информации о требованиях к защите информации и информации, доступ к которой ограничен в соответствии с Законодательством.

Правила обязательны для исполнения Оператором и всеми Субъектами Системы: участниками и операторами услуг платежной инфраструктуры.

Настоящие Правила действуют на территории Российской Федерации. За пределами Российской Федерации настоящие Правила действуют в части, не противоречащей нормам международного законодательства, законам и нормативно-правовым актам иностранных

государств, на территории которых оказываются платежные услуги, и условиям двусторонних договоров, заключенных Оператором с Субъектами Системы (ОУПИ и Участниками).

Настоящие Правила включают в себя следующие приложения, являющиеся неотъемлемой частью Правил:

- Приложение № 1 – Форма заявления на участие;
- Приложение № 2 – Условия Оказания Услуги;
- Приложение № 3 – Тарифы;
- Приложение № 4 – Порядок обеспечения БФПС;
- Приложение № 5 – Регламент СЭДО ПС СБК;
- Приложение №6 – План ОНиВД.

Оператор вправе в одностороннем порядке вносить изменения в Правила.

Оператор обеспечивает Субъектам Системы возможность предварительного ознакомления с предполагаемыми изменениями Правил и направления ими своего мнения Оператору в течение одного месяца со дня размещения проекта изменений на официальном сайте Оператора. Оператор уведомляет Субъекты Системы путем размещения соответствующего уведомления на официальном сайте или иным доступным образом. При этом срок введения в действие, утвержденных Оператором, изменений Правил не может быть менее одного месяца с даты окончания срока, отведенного на ознакомление и направление Субъектами своего мнения Оператору.

1.3. Конфиденциальность.

Под конфиденциальной информацией понимается информация ограниченного доступа, в том числе составляющая коммерческую тайну Субъектов Системы, инсайдерская информация, а также любая иная принадлежащая Субъекту Системы информация независимо от формы ее предоставления, передаваемая раскрывающей стороной принимающей стороне. Любые отчеты, анализы или справки, основанные на конфиденциальной информации или содержащие ее, также являются конфиденциальными и признаются конфиденциальной информацией.

Оператор и Субъекты взаимно гарантируют сохранение конфиденциальности получаемых и передаваемых в рамках Системы данных, информации, документов (в том числе договора участия), программного обеспечения, кодов и паролей, персональных данных клиентов, любой информации об операциях Участника в рамках Системы , а также иной информации, составляющей коммерческую или иную охраняемую законом тайну.

Оператор и Субъекты гарантируют соблюдение банковской тайны в соответствии с законодательством Российской Федерации и законодательствами стран деятельности иностранных участников.

Для обеспечения конфиденциальности и целостности информации в рамках деятельности в Системе Субъекты Системы обязаны использовать закрытые каналы связи. Передача конфиденциальной информации по открытым каналам связи запрещена.

Принимающая сторона не вправе без письменного согласия (разрешения) раскрывающей стороны разглашать или иным образом раскрывать конфиденциальную информацию третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации и Правилами.

Субъекты Системы принимают на себя обязательства сохранять конфиденциальность информации, используемой и получаемой при осуществлении деятельности в Системе, и вправе, без предварительного письменного согласия раскрывающей стороны, по своему усмотрению и с учетом разумной необходимости передавать ее своим работникам, которым такая информация необходима для работы в Системе и которые допущены к работе с конфиденциальной информацией.

Принимающая сторона несет ответственность за действия (бездействие) своих работников и иных лиц, получивших доступ к конфиденциальной информации.

Принимающая сторона несет ответственность за разглашение конфиденциальной информации, а также за несанкционированное использование конфиденциальной информации, произошедшие по вине принимающей стороны.

Субъекты Системы соглашаются, что деятельность Оператора и операторов услуг платежной инфраструктуры по обработке и хранению информации в рамках деятельности Системы не нарушает их права в отношении такой информации и требований к конфиденциальности.

Субъекты Системы обязуются без предварительного письменного согласия Оператора не разглашать третьим лицам информацию о наличии и (или) содержании программных, технических и иных решений, предназначенных для работы в Системе.

В случае выхода раскрывающей стороны (Субъекта Системы) из Системы, а также в любое время по требованию раскрывающей стороны принимающая сторона обязана будет возвратить раскрывающей стороне по акту всю ранее переданную ей конфиденциальную информацию, а также все копии, любые отчеты, анализы, справки, выписки, репродукции и иные материалы, содержащие конфиденциальную информацию (как в письменной, так и в электронной форме), находящуюся в ее владении и во владении лиц, которым конфиденциальная информация была раскрыта в соответствии с условиями Правил, в течение 5 (пяти) рабочих дней со дня получения уведомления раскрывающей стороны о возврате ей конфиденциальной информации, а в случае невозможности передачи - уничтожить ее (их) и предоставить раскрывающей стороне акт об уничтожении в течение 5 (пяти) рабочих дней со дня получения уведомления раскрывающей стороны об уничтожении конфиденциальной информации. В случае невозможности возврата и (или) уничтожения конфиденциальной информации в сроки, установленные выше, данный срок вправе быть изменен по соглашению сторон.

В случае выхода Субъекта Системы из Системы по любому основанию обязательства по неразглашению конфиденциальной информации сохраняются в течение 5 (пяти) лет со дня выхода Субъекта Системы из Системы.

1.4. Товарные знаки, знаки обслуживания, логотипы и их использование.

Только Оператор может быть правообладателем товарных знаков и знаков обслуживания Системы, предназначенных для индивидуализации продуктов и услуг Системы. Оператор определяет требования и стандарты для использования товарных знаков, знаков обслуживания и логотипов Системы.

Участники обязаны соблюдать требования и стандарты использования товарных знаков, знаков обслуживания и Логотипов Системы и немедленно прекратить любое использование товарных знаков, знаков обслуживания и логотипов Системы в случае прекращения участия в Системе.

Присоединяясь к Правилам, Участник предоставляет Оператору право использовать наименование Участника, товарные знаки и знаки обслуживания Участника, правообладателем которых он является, в целях рекламы и продвижения услуг Системы без взимания какой-либо платы. Оператор обязуется прекратить любое использование в рекламных целях наименования Участника, товарных знаков и знаков обслуживания Участника в случае прекращения участия Участника в Системе.

1.5. Предоставление Субъектами Системы Оператору информации о своей деятельности.

1.5.1. Участники предоставляют Оператору информацию о своей деятельности:

1) при направлении Участником Оператору заявления на участие в Системе;
2) при информировании Оператора об изменении фактического местонахождения, наименования Участника, а также о смене единоличного исполнительного органа Участника - в течение недели после вступления в силу таких изменений;
3) при смене контактной информации Участника: почтового адреса, номеров телефонной связи, адресов электронной почты - в течение недели после вступления в силу таких изменений;
4) по запросу Оператора информации по применяемым Участником процедурам в области ПОД/ФТ/ФРОМУ в случаях, когда предоставление такой информации не противоречит Законодательству - в течение недели после получения Участником соответствующего запроса Оператора;
5) по запросу Оператором финансовой отчетности Участника - в течение недели после получения Участником соответствующего запроса Оператора;
6) регулярно для целей анализа обеспечения в Системе защиты информации при осуществлении переводов денежных средств и расчета показателей уровня риска информационной безопасности, - на ежеквартальной основе не позднее пятнадцатого рабочего дня месяца, следующего за отчетным кварталом;
7) по итогам проведения оценки соответствия уровням защиты информации - в течение недели после завершения оценки соответствия);

8) по запросу Оператора в целях управления рисками Системе - в течение недели после получения Участником соответствующего запроса Оператора;
9) по запросу Оператора о предоставлении информации, касающейся деятельности Участника в качестве субъекта Системы для целей оценки рисков и влияния на БФПС в Системе - в течение недели после получения Участником соответствующего запроса Оператора;
10) по запросу Оператора о предоставлении информации, касающейся деятельности Участника в качестве субъекта Системы в связи с инцидентом БФПС - в срок, указанный в соответствующем запросе Оператора;
11) при осуществлении Оператором контроля за соблюдением Правил Участниками – в течение недели после получения Участником соответствующего запроса Оператора;
12) в порядке и случаях, предусмотренных законодательством Российской Федерации – в течение недели после получения Участником соответствующего запроса Оператора.

Информация предоставляется Участником оперативно:

1) в случае возникновения обстоятельств, препятствующих оказанию Услуг, в день возникновения таких обстоятельств - незамедлительно;
2) в случае выявления Участником в рамках Системы чрезвычайных ситуаций, в том числе, событий, вызвавших системные сбои - незамедлительно;
3) по запросу Оператора информации, касающейся переводов денежных средств, осуществленных Участником в рамках Системы, немедленно по первому требованию;
4) в случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе, не несущего финансовых последствий, но затрагивающего технологические участки, - в срок не позднее 24 часов с момента возникновения (выявления) инцидента, а также в течение 24 часов после его устранения;
5) в случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе несущего финансовые последствия - незамедлительно, не позднее одного часа с момента выявления инцидента;
6) при воздействии обстоятельств непреодолимой силы - в течение одного рабочего дня с момента возникновения указанных обстоятельств в устной форме и в течение трех рабочих дней в письменной форме;

1.5.2. Для предоставления информации Субъекты Системы используют:
1) СЭДО ПС СБК (Приложение № 5) — основной канал обмена ЭД;
2) электронную почту;
3) документы на бумажных носителях.

Использование электронной почты и бумажных документов допускается как резервные каналы в случаях, предусмотренных Приложением № 5 (включая первичный или внеплановый обмен сертификатами ключей проверки ЭП, форс-мажор).

1.5.3. Контактная информация Оператора предоставляется Участнику до начала работы в Системе. В случае изменения контактной информации Оператор уведомляет об этом Участников путем направления уведомления в письменном или электронном виде.

## 2. ОПЕРАТОР

2.1. Оператором является Общество с ограниченной ответственностью “Оператор банковской кооперации” (ООО “Оператор банковской кооперации”), зарегистрированное Банком России в качестве оператора платежной системы в реестре операторов платежных систем за номером 46 от 23.01.2018 г.

2.2. В рамках Платежной Системы Оператор также выполняет функции платежно-клирингового центра.

2.3. Обязанности Оператора.

Оператор обязан:

- определять Правила Системы, организовывать и осуществлять контроль за их соблюдением Субъектами Системы;
- осуществлять привлечение операторов услуг платежной инфраструктуры, обеспечивать контроль за оказанием услуг платежной инфраструктуры участникам;
- вести перечень операторов услуг платежной инфраструктуры и участников;
- организовать систему управления рисками в Системе, осуществлять оценку и управление рисками в Системе, обеспечивать бесперебойность функционирования Системы в соответствии с требованиями законодательства Российской Федерации;
- обеспечить бесперебойность функционирования Платежной Системы в порядке, установленном Банком России;
- определять и внедрять порядок обеспечения бесперебойности функционирования платежной системы (БФПС) в соответствии с требованиями законодательства Российской Федерации и нормативных актов Банка России, включая установление ключевых индикаторов риска, пороговых уровней показателей БФПС и регламентов выполнения процедур;
- обеспечивать соблюдение Субъектами Системы порядка обеспечения БФПС и осуществлять контроль за его выполнением;
- информировать Банк России и участников о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в день такого приостановления (прекращения) в порядке, установленном Банком России;
- определить требования к обеспечению защиты информации в платежной системе;
- создать систему выявления и мониторинга переводов денежных средств без добровольного согласия клиента в платежной системе на основе признаков осуществления операций без добровольного согласия клиента и определить порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента для Участников Системы;

- обеспечивать возможность досудебного рассмотрения споров с Субъектами Системы;
- обеспечивать сохранение банковской тайны, защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации;
- размещать Правила и тарифы на своём официальном сайте;
- обеспечивать выполнение иных обязанностей, предусмотренных Правилами, заключенными договорами с Субъектами Системы, законодательством Российской Федерации.

2.4. Права Оператора.

Оператор имеет право:

- в одностороннем порядке вносить изменения в настоящие Правила в соответствии с требованиями законодательства и порядком, предусмотренными Правилами;
- внедрять новые виды услуг, устанавливать и изменять условия оказания услуг;
- устанавливать и изменять показатели и ключевые индикаторы риска для обеспечения БФПС;
- проводить оценку качества функционирования операционных и технологических средств, информационных систем Системы с привлечением независимых организаций;
- требовать от Субъектов Системы предоставления информации, необходимой для оценки рисков и обеспечения БФПС;
- запрашивать информацию о деятельности Субъектов Системы и требовать ее предоставления в надлежащие сроки;
- осуществлять контроль за соблюдением Субъектами Системы настоящих Правил в пределах их обязанностей и ответственности, закрепленных в Правилах;
- принимать решение о начале или прекращении участия в Системе отдельных участников в соответствии с настоящими Правилами;
- устанавливать и изменять плату и/или тарифы за перевод по всем или отдельным услугам в соответствии с настоящими Правилами;
- определять вознаграждение участника;
- рассматривать жалобы клиентов Участников на действия (бездействие) Участников при оказании Услуги Участниками;
- применять к Участникам и Операторам Услуг Платежной Инфраструктуры (в случае привлечения Оператором сторонних Операторов Услуг Платежной Инфраструктуры) санкции, предусмотренные Правилами;
- принимать участие в рассмотрении споров между Субъектами Системы;
- выносить решения о надлежащем/ненадлежащем оказании Услуги клиенту;
- устанавливать для Участника лимиты на сумму отправления одного перевода денежных средств или общую сумму переводов денежных средств, отправляемых Участником за определенный период времени;

- устанавливать и изменять требования по защите информации при осуществлении перевода денежных средств;
- устанавливать обязательные для Субъектов Системы требования по противодействию отмыванию доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения в соответствии с законодательством Российской Федерации;
- получать от Участников, хранить и передавать Участникам данные клиентов, в том числе персональные, полученные в результате идентификации клиента Участником;
- пользоваться иными правами, предусмотренными Правилами, заключенными договорами с Субъектами Системы, законодательством Российской Федерации.

2.5. Обязанности Оператора в качестве платежно-клирингового центра.

Действуя в качестве платежно-клирингового центра, Оператор обязан:

- осуществлять свою деятельность в соответствии с Правилами и на основании договоров, заключаемых с Расчетными центрами;
- обеспечить прием к обработке и исполнению исходящих операций участников в соответствии с Правилами Системы;
- определять клиринговые позиции (на нетто-основе); формировать и направлять расчетным центрам реестры операций, реестры нетто-позиций, содержащие суммы клиринговых позиций участников, и иную информацию. Формы, состав и порядок предоставления реестров определяются договором с Расчетным центром;
- принимать в отношении Участников, финансовое состояние которых свидетельствует о повышенном риске, ограничительные меры, включая уменьшение лимитов межбанковских расчетов в Системе, а также иные меры, направленные на защиту интересов других Участников и обеспечение БФПС;
- формировать и направлять Участникам отчеты, формы, состав и порядок предоставления которых определены Правилами Системы или внутрисистемными документами;
- нести ответственность за убытки, причиненные вследствие неоказания и (или) ненадлежащего оказания платежных клиринговых услуг;
- обеспечивать сохранение банковской тайны, защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации.

2.6. Оператор вправе привлечь для обслуживания Участников несколько операторов услуг платежной инфраструктуры - расчетных центров и операционных центров.

Организация, заинтересованная в оказании услуг оператора услуг платежной инфраструктуры Участникам, сообщает об этом Оператору. Оператор осуществляет проверку организации на соответствие требованиям, установленным Правилами, и принимает соответствующее решение.

Требования к операторам услуг платежной инфраструктуры объективны и обеспечивают равноправный доступ операторов услуг платежной инфраструктуры в Платежную Систему.

Оператор устанавливает следующие требования к финансовому состоянию операторов услуг платежной инфраструктуры:

- Положительная величина чистых активов;
- Отсутствие просроченной задолженности по платежам в бюджет;
- Отсутствие фактов осуществления процедур банкротства или санации;
- Соблюдение установленных обязательных нормативов (в случае, если применимо к конкретному оператору услуг платежной инфраструктуры);
- Предоставление Оператору по запросу финансовой отчетности, если она не находится в публичном доступе.

Оператор устанавливает следующие требования к технологическому обеспечению операторов услуг платежной инфраструктуры:

- Наличие программно-аппаратного комплекса, реализующего функционал услуг платежной инфраструктуры Системы и функционирующего во временных интервалах сеансов обработки, установленных Правилами;
- Наличие комплексной системы обеспечения информационной безопасности, в том числе средств антивирусной защиты;
- Наличие средств коммуникации для информационного обмена с Оператором и Субъектами Системы.

2.7. Оператор ведет перечень операторов услуг платежной инфраструктуры.

Перечень включает в себя следующую информацию по каждому оператору услуг платежной инфраструктуры:

- наименование оператора услуг платежной инфраструктуры;
- вид деятельности оператора услуг платежной инфраструктуры в рамках Системы;
- местонахождение (адрес);
- контактный телефон, официальный сайт.

2.8. Оператор ведет перечень Участников.

Перечень включает в себя следующую информацию по каждому Участнику:

- наименование Участника;
- место нахождения (адрес) Участника;
- контактный телефон, адрес официального сайта Участника.

Оператор присваивает каждому Участнику Индивидуальный Код. Код участника является составным и включает:

- признак вида участия (1 – прямое участие, 2 -косвенное участие);
- порядковый номер, присваиваемый Участнику Оператором;
- код страны, резидентом которой является Участник;
- национальный банковский идентификационный код (БИК).

Код участника однозначно определяет каждого Участника и вид участия.

## 3. РАСЧЕТНЫЙ ЦЕНТР

Расчетный центр обязан:

- участвовать в Системе в качестве прямого Участника;
- осуществлять свою деятельность в соответствии с заключенным с Оператором договором, настоящими Правилами и на основании договоров банковского счета, заключенных с Участниками;
- исполнять поступившие от платежно-клирингового центра распоряжения Участников Системы посредством списания и зачисления денежных средств по банковским счетам Участников;
- обеспечивать сохранение банковской тайны, защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации;
- предоставлять информацию о своей деятельности в рамках Системы в сроки и объеме, установленные в договоре, заключенном с Оператором;
- обеспечивать соблюдение порядка обеспечения БФПС в части расчетных услуг;
- обеспечивать переход на резервный комплекс программных и технических средств в соответствии с планом обеспечения непрерывности и восстановления деятельности;
- незамедлительно информировать Оператора о возникновении инцидентов, влияющих на оказание расчетных услуг;
- поддерживать техническую готовность к обеспечению взаимозаменяемости при наличии в Системе нескольких Расчетных центров;
- своевременно уведомлять Оператора об изменениях организационно-правовой формы, реорганизации, изменении своего места нахождения и почтового адреса, изменении своих банковских реквизитов, а также о любых других изменениях, которые могут существенным образом отразиться на исполнении своих обязательств, вытекающих из Правил, включая факты банкротства и пр.;
- предоставлять Оператору заверенные надлежащий образом:
    - копию лицензии, в течение 15 (пятнадцати) рабочих дней с даты получения новой лицензии;
    - копии изменений/дополнений в Устав или Устава в новой редакции, свидетельств о внесении соответствующих записей в Единый государственный реестр юридических лиц (ЕГРЮЛ) и (или) копии Листов записи единого государственного реестра юридических лиц о внесении изменений не позднее 15 (пятнадцати) дней с даты регистрации изменений;
    - копии документов, подтверждающих избрание нового Единоличного исполнительного органа, продлении полномочий лица, назначенного на должность Единоличного исполнительного органа, в течение 15 (пятнадцати) дней с даты принятия уполномоченным органом соответствующего решения;

- предоставлять финансовую отчетность ежеквартально, не позднее 15 рабочих дней после нормативно установленных сроков подготовки такой отчетности;
- обеспечивать выполнение иных обязанностей, предусмотренных законодательством Российской Федерации, договором с Оператором, Правилами, а также заключенными договорами с Субъектами Системы.

Расчетный центр имеет право:

- определять порядок и условия открытия и ведения счетов Участников в соответствии с законодательством Российской Федерации и с учетом условий, установленных настоящими Правилами;
- использовать для расчетов с иностранными Участниками счета в иностранных банках, в том числе открытые у Участников;
- пользоваться иными правами, предусмотренными Правилами, заключенными договорами с Субъектами, законодательством Российской Федерации.

Расчетный центр не вправе:

- в одностороннем порядке приостанавливать (прекращать) оказание услуг Участникам, за исключением случаев, предусмотренных Правилами.

## 4. ОПЕРАЦИОННЫЙ ЦЕНТР

Операционный центр обязан:

- осуществлять свою деятельность в соответствии с Правилами Системы и на основании договоров, заключаемых с Оператором и Субъектами Системы;
- обеспечивать гарантированный уровень бесперебойности оказания операционных услуг, в том числе обеспечивать уровень безопасности и защищенности операций в соответствии с требованиями законодательства Российской Федерации;
- обеспечивать обмен электронными сообщениями между Субъектами Системы, в том числе передачу исходящих реестров операций Участников в платежно-клиринговый центр, а также передачу извещений (подтверждений) о приеме и об исполнении исходящих реестров операций Участников;
- обеспечивать сохранение банковской тайны, защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации;
- по распоряжению Оператора приостанавливать или прекращать маршрутизацию авторизационных запросов Участников;
- обеспечивать соблюдение порядка обеспечения БФПС в части операционных услуг;
- незамедлительно информировать Оператора о возникновении инцидентов, влияющих на оказание операционных услуг;
- обеспечивать переход на резервный комплекс программных и технических средств в соответствии с планом обеспечения непрерывности и восстановления деятельности;

- предоставлять информацию о своей деятельности в рамках Системы по запросам Оператора, в сроки и объеме, устанавливаемые в запросах Оператора;
- своевременно уведомлять Оператора об изменениях организационно-правовой формы, реорганизации, изменении своего места нахождения и почтового адреса, изменении своих банковских реквизитов, а также о любых других изменениях, которые могут существенным образом отразиться на исполнении своих обязательств, вытекающих из Правил, включая факты банкротства и пр.;
- предоставлять Оператору заверенные должным образом:
    - копии изменений/дополнений в Устав или Устава в новой редакции, свидетельств о внесении соответствующих записей в Единый государственный реестр юридических лиц (ЕГРЮЛ) и (или) копии Листов записи единого государственного реестра юридических лиц о внесении изменений не позднее 15 (пятнадцати) дней с даты регистрации изменений;
    - копии документов, подтверждающих избрание нового Единоличного исполнительного органа, продлении полномочий лица, назначенного на должность Единоличного исполнительного органа, в течение 15 (пятнадцати) дней с даты принятия уполномоченным органом соответствующего решения;
- предоставлять финансовую отчетность ежеквартально, не позднее 15 рабочих дней после нормативно установленных сроков подготовки такой отчетности;
- нести ответственность за реальный ущерб, причиненный Оператору и Субъектам Системы вследствие неоказания и (или) ненадлежащего оказания операционных услуг;
- осуществлять иные действия, связанные с использованием информационно-коммуникационных технологий, необходимых для функционирования Системы, и обеспечивать выполнение иных обязанностей, предусмотренных Правилами, заключенными договорами с Субъектами Системы, законодательством Российской Федерации.

Операционный центр имеет право:

- на оказание операционных услуг в рамках других платежных систем;
- пользоваться иными правами, предусмотренными Правилами, заключенными договорами с Субъектами, законодательством Российской Федерации.

Операционный центр не вправе:

- в одностороннем порядке приостанавливать (прекращать) оказание операционных услуг Участникам за исключением случаев, предусмотренных Правилами.

## 5. УЧАСТНИКИ

5.1. В Системе допускается прямое и косвенное участие. Участниками Системы могут быть операторы по переводу денежных средств, АО “Почта России” (в качестве косвенного участника) и иностранные национальные почтовые операторы (при наличии лицензии/разрешения на оказание платежных услуг), иностранные банки и финансовые

организации, имеющие лицензии локальных регуляторов на оказание платежных услуг (далее все виды иностранных участников именуются как иностранный банк).

Операторы по переводу денежных средств, включая операторов по переводу электронных денежных средств, осуществляют свою деятельность в соответствии с законодательством Российской Федерации, Правилами и Стандартами Системы.

Иностранные банки осуществляют свою деятельность в качестве Участника Системы в соответствии с национальным законодательством и Правилами Системы.

Специфика национального законодательства страны местонахождения иностранного банка, порядка расчетов и условий сотрудничества учитывается в договоре участия между Оператором и иностранным банком.

5.2. Кредитная организация для участия в Системе должна соответствовать следующим критериям:

- иметь действующую лицензию Банка России на осуществление банковских операций (для иностранных банков – действующую лицензию национального регулятора);
- соблюдать требования законодательства Российской Федерации (для иностранных банков – национального законодательства) по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- иметь техническое оснащение, соответствующее технологическим требованиям к работе в Системе и Правилам;
- обеспечивать надлежащую защиту информации в соответствии с требованиями законодательства Российской Федерации (для иностранных банков – национального законодательства) и Правил.

Национальные почтовые организации, включая АО «Почта России», привлекаемые к участию в Системе, должны соответствовать тем же критериям кроме наличия банковской лицензии.

5.3. Участник обязан:

- осуществлять свою деятельность в соответствии с Правилами, а также в соответствии с условиями и на основании договоров, заключенных с Оператором и операторами услуг платежной инфраструктуры; обеспечивать выполнение требований Правил, договоров с Субъектами Системы и законодательства Российской Федерации;
- оказывать Услуги в соответствии с перечнем Услуг и условиями их оказания, установленными в договоре участия;
- осуществлять обслуживание клиентов на условиях, установленных Правилами и тарифами Системы; при оказании Услуг не взимать с клиентов никаких дополнительных сборов, за исключением прямо предусмотренных настоящими Правилами;

- обеспечить клиентам возможность ознакомления с Условиями оказания Услуг и доводить до сведения клиентов условия выплаты и ограничения до наступления безотзывности перевода денежных средств;
- обеспечить получение согласия клиента с Условиями оказания Услуг до момента наступления безотзывности перевода денежных средств и по первому требованию Оператора предоставлять Оператору доказательства получения такого согласия;
- обеспечивать наличие на Счете в Расчетном центре денежных средств в размере, достаточном для последующего расчета по операциям, оплаты вознаграждений и комиссий в соответствии с Правилами и тарифами Системы;
- оплачивать услуги, оказываемые Участнику Оператором и ОУПИ в рамках Системы, вознаграждение другим Участникам, установленные Правилами и тарифами Системы, в порядке, определенном Правилами;
- отвечать перед Субъектами Системы по всем обязательствам, вытекающим из совершенных Операций;
- предоставлять Расчетным Центрам право списывать без дополнительного распоряжения Участника со Счета Участника суммы операций, вознаграждения и комиссий в соответствии с Правилами и тарифами Системы на основании реестров платежной системы;
- обеспечивать должный уровень защиты информации, в том числе персональных данных, и полную конфиденциальность в отношении любой информации, связанной с работой Системы, всеми сотрудниками Участника, которые будут непосредственно работать с Системой, а также сотрудниками Участника, которые по должности смогут иметь доступ к документации и информации в связи с работой в Системе;
- применять установленные законодательством процедуры для обеспечения защиты персональных данных клиентов; обеспечить защищенную передачу персональных данных при любой передаче персональных данных; незамедлительно уведомлять Оператора о любых случаях несанкционированного раскрытия персональных данных или несанкционированного доступа к персональным данным; сотрудничать с Оператором по вопросам урегулирования последствий несанкционированного раскрытия персональных данных;
- в случае прекращения участия в Системе незамедлительно стереть или уничтожить персональные данные, полученные Участником в рамках участия в Системе, в соответствии с требованиями законодательства Российской Федерации, за исключением случаев, когда продолжение обработки персональных данных требуется в соответствии с законодательством Российской Федерации;
- не вносить изменений в интерфейсы, телекоммуникации и алгоритмы работы программного обеспечения, используемого в Системе, без предварительного письменного уведомления и согласия Оператора;
- выполнять требования Оператора по выявлению и мониторингу переводов денежных средств, осуществляемых без добровольного согласия клиента;
- по первому требованию немедленно предоставлять Оператору любую документацию, касающуюся переводов денежных средств, осуществленных Участником в рамках Системы;

- обеспечить комплекс необходимых мер для контроля за тем, чтобы Система не использовалась клиентами в целях обхода ограничений, установленных законодательством Российской Федерации и органами валютного регулирования, а также с целью легализации (отмывания) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;
- предоставлять по запросу Оператора информацию по процедурам в ПОД/ФТ/ФРОМУ в случаях, когда предоставление такой информации не противоречит действующему законодательству Российской Федерации. Предоставление такой информации может осуществляться в письменном виде, в форме электронных сообщений, в устной форме во время встреч, организуемых представителями Участника или Оператора, путем заполнения Участником специальных анкет, направляемых Оператором Участнику, а также иными согласованными между Участником и Оператором способами;
- соблюдать порядок обеспечения БФПС, установленный Оператором;
- незамедлительно информировать Оператора о возникновении инцидентов, влияющих на функционирование Системы, в сроки, установленные порядком обеспечения БФПС;
- предоставлять Оператору информацию, необходимую для оценки рисков и обеспечения БФПС, в сроки и объеме, установленные настоящими Правилами;
- обеспечивать наличие планов обеспечения непрерывности деятельности и восстановления деятельности;
- нести полную ответственность за действия/бездействие сторонних организаций, привлекаемых Участником для исполнения своих обязанностей при осуществлении деятельности в Системе;
- оказывать Оператору содействие в расследовании спорных ситуаций;
- предоставлять отчетность Оператору в соответствии с Правилами;
- своевременно уведомлять Оператора об изменениях организационно-правовой формы, реорганизации, изменении своего места нахождения и почтового адреса, изменении своих банковских реквизитов, а также о любых других изменениях, которые могут существенным образом отразиться на исполнении Участником своих обязательств, вытекающих из Правил, включая факты банкротства, лишения специального разрешения (лицензии) на осуществление профессиональной деятельности и пр.;
- предоставлять Оператору должным образом заверенные:
    - копию лицензии, не позже 15 (пятнадцати) календарных дней с даты получения новой лицензии;
    - копии изменений/дополнений в Устав или Устава в новой редакции, свидетельств о внесении соответствующих записей в Единый государственный реестр юридических лиц (ЕГРЮЛ) и (или) копии Листов записи единого государственного реестра юридических лиц о внесении изменений не позже 15 (пятнадцати) календарных дней с даты регистрации изменений;
    - копии документов, подтверждающих избрание нового Единоличного исполнительного органа Участника, продлении полномочий лица,

назначенного на должность Единоличного исполнительного органа Участника, не позже 15 (пятнадцати) календарных дней с даты принятия уполномоченным органом соответствующего решения;

- предоставлять финансовую отчетность по запросу Оператора;
- содействовать развитию Системы;
- размещать информационные материалы об участии Участника в Системе при условии согласования содержания и дизайна таких информационных материалов с Оператором; предварительно согласовывать в письменном виде с Оператором любую информацию, публикуемую Участником, в отношении Оператора или Системы (включая, но не ограничиваясь, пресс-релизы и рекламу);
- обеспечить реализацию процессов выявления, идентификации и анализа риска информационной безопасности в отношении объектов информационной инфраструктуры Участника;
- обеспечивать выполнение иных обязанностей, установленных Правилами, Стандартами Системы, заключенными договорами с Субъектами Системы, законодательством Российской Федерации в отношении Участников.

5.4. Косвенный Участник обязан открыть счет у Прямого Участника Системы для учета расчетов с другими Участниками Системы.

5.5. Участник имеет право:

- требовать от Оператора надлежащего исполнения им своих обязательств;
- взимать с клиентов Плату за оказываемые Услуги, если это предусмотрено Условиями оказания Услуг;
- требовать от Оператора уплаты межбанковского вознаграждения за оказание Услуг;
- пользоваться услугами Оператора и операторов услуг платежной инфраструктуры;
- получать консультации Оператора по вопросам функционирования Системы;
- направлять Оператору запросы в отношении жалоб и претензий клиентов, поступивших в адрес Участника;
- вносить предложения по улучшению работы Системы, введению новых услуг в рамках Системы и другим вопросам деятельности Системы;
- пользоваться иными правами, предусмотренными Правилами, заключенными договорами с Субъектам Системы, законодательством Российской Федерации.

5.6. Участник заявляет о заинтересованности в участии в Системе путем предоставления Оператору надлежащим образом оформленного заявления и комплекта документов, указанного в Приложении №1.

Оператор проводит проверку предоставленного заявления и комплекта документов в течение не более, чем 15 (пятнадцати) календарных дней.

В случае отрицательного результата рассмотрения комплекта документов Оператор направляет организации соответствующее уведомление по электронной почте на адрес, указанный в заявлении на участие в Системе.

При положительном результате рассмотрения комплекта документов Оператор в течение 5 (пяти) рабочих дней подготавливает и направляет Заявителю проекта договора участия в Системе. Подписание договора участия является согласием Участника на присоединение к настоящим Правилам. Любой Участник присоединяется к Правилам путем принятия их в целом в соответствии с требованиями части 7 статьи 20 Федерального закона от 27.06.2011 года № 161-ФЗ.

Участник присоединяется к Правилам на 5 (пять) лет с даты начала участия в Системе, указанной в Уведомлении о начале участия. Срок присоединения к Правилам автоматически продлевается на каждый последующий год, если Участник за 90 (девяносто) календарных дней до истечения первоначального пятилетнего срока или последующего годичного периода не вручит письменного извещения Оператору о своем намерении прекратить участие в Системе.

Оператор после подписания договора участия направляет Заявителю уведомление о подтверждении даты начала участия Заявителя в Платежной Системе, которое содержит дату начала участия Заявителя в Системе и номер Участника (далее «Уведомление о начале участия»). Заявитель становится Участником на условиях договора участия и настоящих Правил с даты, указанной в Уведомлении о начале участия.

После получения Уведомления о начале участия Участник приступает к осуществлению переводов денежных средств в рамках Системы после заключения договора с Расчетным центром (Расчетными центрами) и открытия необходимых счетов.

5.7. Прекращение и приостановление участия в Системе возможно по следующим основаниям:

- по инициативе Участника;
- по инициативе Оператора;
- по соглашению сторон;
- в иных случаях, предусмотренных Правилами и законодательством Российской Федерации.

5.8. Участник вправе в одностороннем порядке принять решение о прекращении участия в Системе. В случае принятия такого решения Участник обязан направить Оператору письменное заявление о прекращении Участия в свободной форме.

С даты получения Оператором Заявления о прекращении участия в Системе Оператор принимает меры по блокировке доступа Участника к услугам Системы. Участник обязан до даты прекращения участия:

- исполнить все финансовые и иные обязательства, возникшие у Участника перед всеми Субъектами Системы за период деятельности в Системе в качестве ее Участника;
- передать Оператору всю конфиденциальную информацию в соответствии с Правилами;

- удалить все информационные материалы с товарными знаками, знаками обслуживания и логотипами Системы не позднее 10 (десяти) рабочих дней, следующих за датой направления Заявления о прекращении участия.

Участие в Системе прекращается не ранее 90 (девяноста) календарных дней с даты получения Оператором Заявления о прекращении участия при отсутствии у Участника финансовых обязательств перед всеми Субъектами Системы. После окончания указанного выше срока урегулирования обязательств Оператор письменно уведомляет Расчетный центр о факте прекращения участия в Системе данного Участника в добровольном порядке и отсутствии у него финансовых обязательств.

Прекращение участия в Системе не освобождает Участника от обязательств, возникших в рамках его деятельности в Системе.

5.9. Оператор вправе приостановить работу Участника в Системе в случаях нарушения Участником требований законодательства Российской Федерации, Правил Системы, а также, если Участник не способен (или есть достаточные основания считать его неспособным) выполнять свои обязательства как Участника, в том числе, но не ограничиваясь:

- неисполнения или ненадлежащего исполнения Участником своих обязательств перед Субъектами Системы;
- нанесения вреда деловой репутации Системы;
- невозможности удовлетворения предъявленных к счету Участника в Расчетном центре требований для осуществления расчетов по операциям, в том числе по причине наложения ареста на денежные средства на счете, приостановления операций по счету в соответствии с законодательством Российской Федерации;
- неосуществления Участником всех необходимых мер в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма;
- запрета со стороны Банка России на осуществление отдельных банковских операций, невозможность проведения которых препятствует исполнению обязательств Участника в рамках деятельности в Системе;
- выявления негативных факторов, влекущих риски нарушения Участником бесперебойности функционирования Системы;
- выявления влияющих на безопасность функционирования Системы нарушений Участником требований к обеспечению защиты информации в Системе;
- отсутствие операций у Участника в течение 6 (шести) календарных месяцев подряд.

В случае принятия Оператором решения о приостановлении участия в Системе, Оператор направляет Участнику уведомление о приостановлении его участия в Системе с указанием нарушения, послужившего причиной принятия Оператором решения, в котором также определяется срок устранения нарушения.

Деятельность Участника в Системе возобновляется при условии устранения нарушения, указанного Оператором в уведомлении.

Если нарушение не будет устранено в установленный срок, Оператор вправе инициировать процедуру прекращения участия Участника в Системе.

После принятия решения о прекращении участия Оператор направляет уведомление Участнику, содержащее основание и дату прекращения его участия и предпринимает меры по блокировке доступа к услугам Системы. В период с даты направления Оператором уведомления о прекращении Участия в Системе до даты прекращения участия в Системе Участник обязан:

- исполнить все финансовые и иные обязательства, возникшие у Участника перед всеми Субъектами Системы за период деятельности в Системе в качестве ее Участника;
- передать Оператору всю конфиденциальную информацию в соответствии с Правилами;
- удалить все информационные материалы с товарными знаками, знаками обслуживания и логотипами Системы не позднее 10 (десяти) рабочих дней, следующих за датой получения Уведомления о прекращении участия.

Участие в Системе прекращается не ранее 90 (девяноста) календарных дней с даты получения Участником Уведомления о прекращении участия при отсутствии у Участника финансовых обязательств перед всеми Субъектами Системы. После окончания указанного выше срока урегулирования обязательств Оператор письменно уведомляет Расчетный центр о факте прекращения участия в Системе данного Участника в добровольном порядке и отсутствии у него финансовых обязательств. Расчетный центр осуществляет соответствующие процедуры согласно своим внутренним регламентам.

Прекращение участия в Системе не освобождает Участника от обязательств, возникших в рамках его деятельности в Системе.

Безоговорочными условиями прекращения участия в Системе являются:

- отзыв у Участника лицензии на осуществление банковской деятельности;
- признание Участника банкротом.

## 6. УСЛУГИ ПЛАТЕЖНОЙ СИСТЕМЫ

6.1. Общие положения.

Услуги платежной системы оказываются Участниками их клиентам – физическим и юридическим лицам - в соответствии с законодательством Российской Федерации, национальными законодательствами стран иностранных Участников, настоящими Правилами и Условиями оказания Услуги, которые являются неотъемлемой частью настоящих Правил.

Условия оказания Услуг устанавливаются Оператором и являются едиными для всех Участников на территории Российской Федерации и на территориях действия иностранных Участников. Оператор публикует Условия оказания Услуг на официальном сайте. Оператор вправе вносить изменения в Условия оказания Услуг в порядке, предусмотренном настоящими Правилами.

Оператор вправе устанавливать лимиты на сумму одной операции и совокупную сумму операций за период.

Участник обязан ознакомить клиента с Условиями оказания Услуг, в том числе путем размещения Условий оказания Услуг в свободном для клиентов доступе в отделениях и на электронных носителях, а также получить согласие клиента с Условиями оказания Услуги до момента совершения клиентом перевода денежных средств. По требованию Оператора Участник обязан доказать Оператору получение согласия клиента с Условиями оказания Услуг.

6.2. В рамках Платежной Системы применяются следующие формы безналичных расчетов:

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

6.3. Перевод денежных средств физического лица в пользу физического лица.

Для отправки перевода отправитель (физическое лицо) составляет распоряжение, которое включает сумму и валюту выплаты перевода, номер мобильного телефона получателя и страну, если перевод трансграничный. Распоряжение может быть направлено в Систему через каналы обслуживания Участника, ведущего счет отправителя, или мобильное приложение Системы. Отправленному переводу присваивается КНП (контрольный номер перевода) – уникальный идентификатор перевода в Системе.

Получатель уведомляется Системой о переводе, отправленном в его адрес отправителем, через мобильное приложение Системы или SMS. Получатель имеет возможность отказаться от получения перевода или выбрать удобный для него способ получения: зачислением на банковский счет, банковскую карту или выдачу наличными в отделении Участника Системы.

Для получения перевода наличными получатель в отделении Участника Системы, оказывающего такую услугу, должен предъявить документ, удостоверяющий личность, и КНП для поиска перевода в Системе.

Безотзывность перевода денежных средств для данной услуги наступает с момента списания денежных средств для оплаты отправляемого перевода с банковского счета (или банковской карты) отправителя, либо внесением в кассу наличных.

Безусловность перевода денежных средств для данной услуги наступает с момента выбора получателем способа получения перевода безналичным зачислением, либо выполнением получателем всех условий выплаты перевода наличными.

Окончательность перевода денежных средств для данной услуги наступает с момента зачисления перевода на счет/карту получателя или выдачи получателю перевода наличными.

6.4. Перевод денежных средств физического лица в пользу юридического лица или ИП по инициативе физического лица.

Для отправки перевода отправитель (физическое лицо) составляет распоряжение, которое включает сумму перевода в рублях, номер мобильного телефона получателя (юридического лица), предварительно зарегистрированный в Системе, и назначение перевода.

Получатель мгновенно уведомляется Системой о переводе, отправленном в его адрес отправителем через API Системы. Денежные средства перевода зачисляются Участником, обслуживающим получателя, на его расчетный счет. Получатель имеет возможность вернуть перевод отправителю.

Безотзывность и безусловность перевода денежных средств для данной услуги наступают с момента списания денежных средств для оплаты отправляемого перевода с банковского счета (или банковской карты) отправителя.

Окончательность перевода денежных средств для данной услуги наступает с момента зачисления перевода на расчетный счет получателя.

6.5. Перевод денежных средств физического лица в пользу юридического лица или ИП по инициативе юридического лица или ИП.

Для запроса перевода получатель (юридическое лицо или ИП) составляет распоряжение, которое включает сумму перевода в рублях, номер мобильного телефона отправителя и назначение перевода.

Отправитель (физическое лицо) уведомляется Системой о запросе перевода в пользу получателя (юридического лица), отправленном в его адрес получателем через API Системы. Отправитель может отказаться или оплатить перевод с банковского счета или банковской карты. Денежные средства перевода зачисляются Участником, обслуживающим получателя, на его расчетный счет. Получатель имеет возможность вернуть перевод отправителю.

Безотзывность и безусловность перевода денежных средств для данной услуги наступают с момента списания денежных средств для оплаты отправляемого перевода с банковского счета (или банковской карты) отправителя.

Окончательность перевода денежных средств для данной услуги наступает с момента зачисления перевода на расчетный счет получателя.

6.6. Рассмотрение претензий клиентов.

Претензии предъявляются клиентами в соответствии с Условиями оказания Услуг. Участник вправе самостоятельно предоставлять ответы своим клиентам или передавать их на рассмотрение Оператору. При поступлении претензии Оператору от клиента Участника, направленной непосредственно Оператору или переданной Участником, Оператор вправе запрашивать у Участника документы и информацию, необходимые для ответа на претензию. Если в результате рассмотрения претензии Оператор выявит нарушение Участником настоящих Правил, Оператор вправе применить к Участнику санкции, предусмотренные настоящими Правилами.

## 7. РЕГЛАМЕНТ РАБОТЫ СИСТЕМЫ. ВЗАИМОДЕЙСТВИЕ ОПЕРАТОРА И СУБЪЕКТОВ СИСТЕМЫ

7.1. Время обслуживания клиентов.

Услуги Системы клиентам оказываются с использованием автоматизированных систем Оператора и Субъектов Системы. Услуги, которые доступны клиентам через мобильные приложения Системы, оказываются беспрерывно - 24 часа в сутки, без выходных дней.

Услуги Системы, доступные в сети обслуживания и системах самообслуживания Участников, предоставляются клиентам по временным регламентам, устанавливаемым Участниками.

7.2. Режим работы Оператора и операторов услуг платежной инфраструктуры.

Рабочими днями Оператора и операторов услуг платежной инфраструктуры Системы являются рабочие дни, установленные законодательством Российской Федерации. Рабочее время Оператора - с 10.00 до 18.00 московского времени.

7.3. Отчетный период для осуществления платежного клиринга и расчетов.

В качестве единой шкалы времени для осуществления платежного клиринга и расчетов в Системе принято Московское время.

Отчетный период устанавливается с 00:00:00 до 23:59:59 Московского времени. Если отчетный период не является рабочим днём по законодательству Российской Федерации, то расчеты за данный отчетный период проводятся в ближайший рабочий день.

Расчеты между Субъектами Системы проводится по рабочим дням.

7.4. Платежный клиринг осуществляется Оператором, действующим в качестве платежно-клирингового центра (далее ПКЦ), посредством:

- выполнения процедур приема к исполнению распоряжений Участников, включая проверку соответствия распоряжений Участников установленным требованиям, и определение достаточности денежных средств для исполнения распоряжений Участников;
- определения платежных клиринговых позиций Участников в режиме реального времени;
- передачи Расчетным Центрам для исполнения исключительно принятых распоряжений Участников, обеспеченных денежными средствами для проведения расчетов;
- направления Участникам извещений (подтверждений), касающихся приема к проверке их распоряжений, и извещений (подтверждений), касающихся исполнения или отказа в исполнении распоряжений.

7.5. ПКЦ реализует механизм обеспечения обязательств Участников путем авторизации распоряжений строго в пределах Расчетного Лимита Участника, обеспеченного денежными средствами на счетах Расчетных Центров. Неавторизованные распоряжения не принимаются к исполнению в Системе.

7.6. Расчетный Лимит Участника на начало отчетного периода равен остатку денежных средств на счетах Участника в Расчетных Центрах на конец предыдущего отчетного периода и меняется в течение отчетного периода по мере обработки распоряжений от Участников:

- уменьшается по мере авторизации распоряжений Участника на списание денежных средств, по которым Участник является плательщиком;
- увеличивается по мере:
    - пополнения счета Участника в Расчетном центре за счет входящих внешних перечислений;
    - авторизации распоряжений других Участников, по которым Участник является получателем.

Текущий Расчетный Лимит Участника рассчитывается по формуле:

РЛУ=ВО-Сумм_Списания+Сумм_Поступления, где:

Сумм_Списания - текущая сумма принятых ПКЦ распоряжений Участника, включая комиссии в соответствии с Правилами и тарифами Системы;

Сумм_Поступления - сумма авторизованных ПКЦ распоряжений других Участников на перечисление денежных средств в адрес Участника, в отношении которого формируется лимит.

ВО – входящий остаток, сумма денежных средств на счете Участника в Расчетном Центре на начало отчетного периода.

Лимиты Участников формируются в валютах проведения расчетов.

7.7. По окончании отчетного периода Оператор, выполняя функции ПКЦ, формирует реестр нетто позиций Участников и реестр взаиморасчетов в Системе по межбанковским комиссиям, тарифам Оператора и операторов услуг платежной инфраструктуры и направляет их для проведения расчетов в Системе Расчетным Центрам. Одновременно Оператор направляет Участникам для сверки реестр операций за отчетный период.

7.8. Сводный временной регламент функционирования Системы.

| **Функции** | **Время** | **Исполнитель** |
|---|---|---|
| Прием и обработка распоряжений Участников. | Непрерывно | Оператор (ПКЦ) |
| Обмен информацией о внешних пополнениях счетов Участников между Расчетными Центрами и ПКЦ. | По рабочим дням Расчетного Центра. В течение отчетного периода. | РЦ, Оператор (ПКЦ) |
| Подготовка реестра нетто-позиций, реестра взаиморасчетов по межбанковским комиссиям и тарифам Оператора и операторов услуг платежной инфраструктуры, реестров операций для Участников. | 00:00-08:00 Мск | Оператор (ПКЦ) |
| Передача реестров ПКЦ Расчетным Центрам и Участникам | 08:00-08:30 Мск | Оператор (ПКЦ) |
| Проведение расчетов. Формирование и отправка Участникам выписок. | 08:30-11:00 | РЦ |

7.9. Обеспечение бесперебойности функционирования Системы.

Порядок обеспечения бесперебойности функционирования Системы определяется Приложением № 4 к настоящим Правилам и включает:

- систему управления рисками в Системе;
- управление непрерывностью функционирования Системы;
- организацию взаимодействия Субъектов Системы по обеспечению БФПС;
- контроль за соблюдением порядка обеспечения БФПС.

План ОНиВД содержится в Приложении №6 к настоящим Правилам.

## 8. ЗАЩИТА ИНФОРМАЦИИ

Порядок обеспечения защиты информации в Системе для Субъектов Системы определяет Оператор с учетом требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Оператор определяет требования к обеспечению защиты информации в Системе в отношении следующих мероприятий:

- управление риском информационной безопасности в Системе как одним из видов операционного риска, источниками реализации которого являются недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации, недостатки прикладного программного обеспечения автоматизированных систем и приложений, а также несоблюдение требований к указанным процессам деятельности операторами по переводу денежных средств, являющимися Участниками, и операторами услуг платежной инфраструктуры;
- установление состава показателей уровня риска информационной безопасности в платежной системе;
- реализация операторами по переводу денежных средств, являющимися Участниками Системы, и ОУПИ:
    - механизмов, направленных на соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств, и контроль их соблюдения операторами по переводу денежных средств, являющимися Участниками, и ОУПИ;
    - процессов выявления, идентификации и анализа риска информационной безопасности в платежной системе в отношении объектов информационной инфраструктуры Участников, и ОУПИ;
    - процессов реагирования на инциденты защиты информации и восстановления штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации;
    - взаимодействия при обмене информацией об инцидентах защиты информации;
    - мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента, определенных пунктами 4.5 и 4.8 Указания Банка России от 19 августа 2024 года № 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 N 161-ФЗ "О национальной платежной системе", а также о порядке реализации ими мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента», зарегистрированного Министерством юстиции Российской Федерации 04 октября 2024 года № 79704.;

- реализация Оператором процессов применения в отношении операторов по переводу денежных средств, являющихся Участниками, и ОУПИ ограничений по параметрам операций по осуществлению переводов денежных средств в случае выявления факта превышения значений показателей уровня риска информационной безопасности в платежной системе, в том числе условий снятия таких ограничений.

8.1 Информация, подлежащая защите при осуществлении переводов денежных средств.

Требования к обеспечению защиты информации применяются для обеспечения защиты следующей информации (далее - защищаемая информация):

- остатки денежных средств на банковских счетах;
- совершенные переводы денежных средств, в том числе информация, содержащаяся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников, а также в извещениях (подтверждениях), касающихся исполнения распоряжений Участников;
- распоряжения клиентов Участников, Участников и платежно-клирингового центра;
- электронные сообщениях, передаваемые при взаимодействии Субъектов Системы;
- платежные клиринговые позиции;
- реестры, сформированные на основе электронных сообщений;
- информация, необходимая для удостоверения клиентами права распоряжения денежными средствами, в том числе данные держателей платежных карт;
- информация, используемая для идентификации, аутентификации и авторизации сотрудников Участников при осуществлении переводов денежных средств;
- ключевая информация средств криптографической защиты информации (СКЗИ), используемых при осуществлении переводов денежных средств;
- конфигурация, определяющая параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Участником или ОУПИ, используемых для осуществления переводов денежных средств (далее – объекты информационной инфраструктуры);
- конфигурация, определяющей параметры работы технических средств по защите информации;
- информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемая при осуществлении переводов денежных средств.

8.2 Требования к обеспечению защиты информации при осуществлении переводов денежных средств предъявляются

- к организации (или назначению существующего) подразделения, ответственного за организацию и контроль обеспечения защиты информации (далее - служба информационной безопасности), и его функционированию;
- к защите информации на стадиях жизненного цикла объектов информационной инфраструктуры;
- к защите информации при назначении и распределении функциональных прав и обязанностей (далее - ролей) лиц, связанных с осуществлением переводов денежных средств;
- к защите информации при осуществлении доступа к объектам информационной инфраструктуры, включая требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от несанкционированного доступа;
- к защите информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код);
- к защите информации при использовании информационно-телекоммуникационной сети Интернет (далее - сеть Интернет) при осуществлении переводов денежных средств;
- к защите информации при использовании СКЗИ;
- к использованию взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (далее - технологические меры защиты информации);
- к защите среды виртуализации при осуществлении переводов денежных средств Участником или ОУПИ;
- к осведомленности работников Участника или ОУПИ и клиентов (далее - повышение осведомленности) в области обеспечения защиты информации;
- к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагированию на них и восстановлению штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации, а также мероприятий по реализации взаимодействия при обмене информацией об инцидентах защиты информации;
- к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- к совершенствованию Оператором, Участником, ОУПИ защиты информации при осуществлении переводов денежных средств;
- к оценке выполнения Оператором, Участником, ОУПИ требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- к доведению Участником, ОУПИ до Оператора информации об обеспечении в Системе защиты информации при осуществлении переводов денежных средств;

- к противодействию осуществлению переводов денежных средств без добровольного согласия клиента;
- к управлению риском информационной безопасности, а также выявлению и идентификации риска информационной безопасности Участником ОУПИ.

8.3 Способы выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств.

Выполнение требований обеспечивается путем

1) организационных мер защиты информации:
- определения во внутренних документах Субъектов Системы порядка применения организационных мер защиты информации;
- определения лиц, ответственных за применение организационных мер защиты информации;
- исполнения организационных мер защиты;
- организации контроля за исполнением организационных мер защиты информации.

2) использования технических средств защиты информации:
- определения во внутренних документах Субъектов Системы порядка использования технических средств защиты информации, включающего информацию о конфигурации, определяющую параметры работы технических средств защиты информации;
- назначения лиц, ответственных за использование технических средств защиты информации;
- применения избранных технических средств защиты информации;
- организации контроля за использованием технических средств защиты информации.

8.4 К организации и функционированию службы информационной безопасности предъявляются следующие требования:

1) Субъекты Системы
- обеспечивают формирование службы информационной безопасности, в том числе путём возложения функций службы на существующие подразделения;
- определяют во внутренних документах цели и задачи деятельности этой службы;
- предоставляют полномочия и выделяют ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач.

2) Для планирования и контроля обеспечения защиты информации при осуществлении переводов денежных средств Служба информационной безопасности наделяется следующими полномочиями:
- осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- определять требования к техническим средствам защиты информации и организационным мерам защиты информации;

- контролировать выполнение работниками требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, формировать предложения по совершенствованию защиты информации;
- участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации при восстановлении предоставления услуг Системы после сбоев и отказов в работе объектов информационной инфраструктуры.

8.5 К обеспечению защиты информации на стадиях жизненного цикла объектов информационной инфраструктуры Субъекта Системы предъявляются следующие требования:

- включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- участие службы информационной безопасности в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры;
- контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий;
- наличие эксплуатационной документации на используемые технические средства защиты информации и контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации;
- восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе;
- запрет использования защищаемой информации на стадии создания объектов информационной инфраструктуры;
- запрет несанкционированного копирования защищаемой информации на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры;
- защита резервных копий защищаемой информации;
- уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, Правилами и (или) договорами, заключенными Субъектом Системы;
- уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления.

5. К назначению и распределению Субъектом Системы ролей лиц, связанных с осуществлением переводов денежных средств, предъявляются следующие требования:

- регистрацию лиц, 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 по осуществлению переводов денежных средств;

- регистрация сотрудников, обладающих правами по формированию электронных сообщений, содержащих распоряжения об осуществлении переводов денежных средств (далее - электронные сообщения).
- запрет выполнения одним лицом в один момент времени эксплуатации и (или) контроля эксплуатации объекта информационной инфраструктуры, в том числе автоматизированных систем, одновременно с использованием по назначению объекта информационной инфраструктуры в рамках осуществления переводов денежных средств; - запрет выполнения одним лицом в один момент времени создания и (или) модернизации объекта информационной инфраструктуры одновременно с использованием по назначению объекта информационной инфраструктуры в рамках осуществления переводов денежных средств;
- запрет выполнения одним лицом в один момент времени эксплуатации средств и систем защиты информации одновременно с контролем эксплуатации средств и систем защиты информации;
- обеспечение контроля и регистрации действий лиц, которым назначены роли, определенные в настоящем пункте, в том числе эксплуатационного персонала;

8.7 К защите информации при осуществлении доступа к объектам информационной инфраструктуры предъявляются следующие требования:

- идентификация и учет объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации;
- доступ сотрудников под уникальными и персонифицированными учетными записями;
- контроль соответствия активных учетных записей фактическому составу легальных субъектов доступа;
- контроль отсутствия незаблокированных учетных записей уволенных сотрудников, либо сотрудников, отсутствующих на рабочем месте более 30 календарных дней, либо сотрудников внешних (подрядных) организаций, прекративших свою деятельность в организации;
- контроль отсутствия незаблокированных учетных записей неопределенного целевого назначения;
- применение некриптографических средств защиты информации от несанкционированного доступа, в том числе имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности;
- четкое определение правил предоставления и блокирования доступа; хранение эталонной информации о предоставленных правах доступа и обеспечение целостности этой информации;
- исключение бесконтрольного самостоятельного расширения сотрудниками предоставленных им прав доступа;
- исключение бесконтрольного изменения сотрудниками параметров настроек средств и систем защиты информации, параметров настроек автоматизированных систем, связанных с защитой информации;

- назначение сотрудникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации;
- контроль необходимости отзыва прав доступа у сотрудников при изменении их должностных обязанностей;
- контроль прекращения предоставления доступа и блокирование учетных записей при истечении срока предоставления доступа;
- регистрация выполнения сотрудниками ряда неуспешных последовательных попыток аутентификации;
- регистрация осуществления сотрудниками идентификации и аутентификации;
- регистрация авторизации, завершения и (или) прерывания (приостановки) осуществления доступа сотрудниками;
- регистрация изменений аутентификационных данных, используемых для осуществления доступа;
- регистрация действий клиентов, выполняемых с использованием программного обеспечения, входящего в состав объектов информационной инфраструктуры и используемого для осуществления переводов денежных средств;
- регистрация действий, связанных с предоставлением доступа клиентам к системам самообслуживания;
- регистрация действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов;
- принятие и фиксация во внутренних документах решений о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для: контроля физического доступа к объектам информационной инфраструктуры, сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, а также доступа в здания и помещения, в которых они размещаются;
- предотвращение физического воздействия на средства вычислительной техники и телекоммуникационное оборудование, эксплуатация которых обеспечиваются Субъектом Системы и которые используются для осуществления переводов денежных средств, сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств;
- контроль за применением организационных мер защиты информации и (или) использованием указанных технических средств защиты информации;
- принятие мер, направленных на предотвращение хищений носителей защищаемой информации;
- обеспечение возможности приостановления (блокирования) клиентом приема к исполнению распоряжений об осуществлении переводов денежных средств от имени указанного клиента.

8.8 К защите Субъектом Системы информации от воздействия вредоносного кода предъявляются следующие требования:

- защита от вредоносного кода на уровне физических АРМ;

- защита от вредоносного кода на уровне виртуальной информационной инфраструктуры;
- защита от вредоносного кода на уровне серверного оборудования;
- защита от вредоносного кода на уровне контроля межсетевого трафика;
- защита от вредоносного кода на уровне контроля почтового трафика;
- защита от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации;
- функционирование средств защиты от вредоносного кода в постоянном, автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных, на АРМ сотрудников в резидентном режиме с автоматическим запуском при загрузке операционной системы;
- применение средств защиты от вредоносного кода, реализующих функцию контроля целостности их программных компонентов;
- контроль отключения и своевременного обновления средств защиты от вредоносного кода;
- выполнение еженедельных полных проверок на отсутствие вредоносного кода на объектах информационной инфраструктуры;
- использование средств защиты от вредоносного кода различных производителей как минимум для уровней физических АРМ сотрудников, серверного оборудования, контроля межсетевого трафика;
- запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети интернет;
- выполнение проверок на отсутствие вредоносного кода путем анализа информационных потоков между сегментами контуров безопасности и иными внутренними вычислительными сетями Субъекта Системы.
- выполнение предварительных проверок на отсутствие вредоносного кода устанавливаемого или изменяемого программного обеспечения, а также выполнение проверки после установки и (или) изменения программного обеспечения;
- регистрация операций по проведению проверок на отсутствие вредоносного кода; фактов выявления вредоносного кода; неконтролируемого использования технологии мобильного кода; сбоев в функционировании средств защиты от вредоносного кода; сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода; отключения средств защиты от вредоносного кода; нарушения целостности программных компонентов средств защиты от вредоносного кода;
- формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода.

В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Субъект Системы

- обеспечивает принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода;
- при необходимости приостанавливает осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом;

- информирует Оператора в срок, не превышающий 24 часа с момента обнаружения факта воздействия вредоносного кода, о факте воздействия вредоносного кода и о действиях, предпринимаемых для ликвидации последствий.

Оператор в свою очередь информирует другие Субъекты Системы о факте воздействия вредоносного кода и о действиях, предпринимаемых для ликвидации последствий.

8.9 К защите Субъектом Системы информации при использовании сети интернет для осуществления переводов денежных средств предъявляются следующие требования:

- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения доступа
- к содержанию защищаемой информации, передаваемой по сети интернет;
- к защищаемой информации на объектах информационной инфраструктуры с использованием сети интернет;
- к защищаемой информации путем использования уязвимостей программного обеспечения;
- фильтрация сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью интернет.

Участник обеспечивает клиентов рекомендациями по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети интернет.

8.10 Защита информации при осуществлении переводов денежных средств с использованием СКЗИ осуществляется в следующем порядке:

1) Работы по обеспечению защиты информации с помощью СКЗИ проводятся 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 (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66, зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года N 6382, 25 мая 2010 года N 17350 («Бюллетень нормативных актов федеральных органов исполнительной власти» от 14 марта 2005 года N 11, от 14 июня 2010 года № 24), и технической документацией на СКЗИ.
2) В случае если Субъект Системы применяет СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа.
3) Субъект Системы применяет СКЗИ, которые:

- допускают встраивание СКЗИ в технологические процессы осуществления переводов денежных средств, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

- поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
- поддерживают непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

4) В случае применения СКЗИ Субъект Системы определяет во внутренних документах и выполняет порядок применения СКЗИ, включающий:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления переводов денежных средств;
- порядок эксплуатации СКЗИ и 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.

5) Криптографические ключи изготавливаются клиентом (самостоятельно), Субъектом Системы.
6) Безопасность процессов изготовления криптографических ключей СКЗИ обеспечивается комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.
7) Оператор определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации.

8.11 Защита информации с использованием технологических мер защиты информации осуществляется в следующем порядке:

- Субъекты Системы обеспечивают учет и контроль состава, установленного и (или) используемого на средствах вычислительной техники программного обеспечения;
- Оператор определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств, а Субъекты Системы обеспечивают выполнение указанного порядка;

- Распоряжение клиента, распоряжение Участника и распоряжение ЦПКК в электронном виде может быть удостоверено электронной подписью, а также в соответствии с пунктом 3 статьи 847 Гражданского кодекса Российской Федерации аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом.
- При эксплуатации объектов информационной инфраструктуры Субъекты Системы обеспечивают:
    - защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации;
    - контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры;
    - аутентификацию входных электронных сообщений;
    - взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями;
    - восстановление информации об остатках денежных средств на банковских счетах и данных держателей платежных карт в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;
    - сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчетов в Системе;
    - выявление фальсифицированных электронных сообщений, в том числе осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации.

8.12 К защите среды виртуализации при осуществлении переводов денежных средств, предъявляются следующие требования:

- Субъекты Системы обеспечивают разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ сотрудников только в пределах одного контура безопасности (при наличии более одного контура безопасности);
- Субъекты Системы обеспечивают разграничение и контроль осуществления одновременного доступа виртуальных машин к системе хранения данных в пределах контура безопасности;
- Субъекты Системы обеспечивают идентификацию и аутентификацию пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам;

- Субъекты Системы обеспечивают возможность принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной;
- Субъекты Системы обеспечивают контроль и протоколирование доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных с реализацией двухфакторной аутентификации; размещение средств защиты информации, используемых для организации контроля и протоколирования доступа сотрудников к серверным компонентам виртуализации и системе хранения данных на физических СВТ; размещение серверных и пользовательских компонентов объектов информационной инфраструктуры на разных виртуальных машинах;
- В случае наличия более одного контура безопасности Субъекты Системы обеспечивают выделение в вычислительных сетях отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения серверных компонент объектов информационной инфраструктуры, включенных в разные контуры безопасности; выделение в вычислительных сетях отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения АРМ сотрудников, включенных в разные контуры безопасности; организацию межсетевого экранирования вышеуказанных сегментов (групп сегментов) вычислительных сетей, включая фильтрацию данных на сетевом и прикладном уровнях; реализацию контроля информационного взаимодействия между вышеуказанными сегментами (группами сегментов) вычислительных сетей в соответствии с установленными правилами и протоколами сетевого взаимодействия;
- Субъекты Системы обеспечивают регламентацию и контроль выполнения операций в рамках жизненного цикла базовых образов виртуальных машин и операций по копированию образов виртуальных машин; включение в базовые образы виртуальных машин только программного обеспечения технических мер защиты информации, применяемых в пределах виртуальных машин и программного обеспечения автоматизированных систем; отнесение каждой из виртуальных машин только к одному из контуров безопасности; запрет на копирование текущих образов виртуальных машин, использующих СКЗИ, с загруженными криптографическими ключами; контроль завершения сеанса работы пользователей с виртуальными машинами;
- Субъекты Системы обеспечивают регистрацию операций, связанных с: запуском (остановкой) виртуальных машин; изменением параметров настроек виртуальных сетевых сегментов, реализованных средствами гипервизора; созданием и удалением виртуальных машин; созданием, изменением, копированием, удалением базовых образов виртуальных машин; копированием текущих образов виртуальных машин; изменением прав логического доступа к серверным компонентам виртуализации; изменением параметров настроек серверных компонентов виртуализации; аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации; аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам; параметров настроек технических средств защиты информации, используемых для реализации

контроля доступа к серверным компонентам виртуализации; изменением настроек технических средств защиты информации, используемых для обеспечения защиты виртуальных машин.

8.13 К осведомленности в области обеспечения защиты информации предъявляются следующие требования:

1) Субъекты Системы обеспечивают повышение осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации и порядку использования технических средств защиты информации.
2) Субъекты Системы обеспечивают повышение осведомленности работников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации.
3) 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.

8.14 Выявление инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств. Реагирование на них и восстановление штатного функционирования объектов информационной инфраструктуры. Мероприятия по взаимодействию при обмене информацией об инцидентах.

1) Оператор определяет требования к порядку, форме и срокам информирования Оператора и Субъектов Системы о выявленных в Системе инцидентах защиты информации и к взаимодействию Оператора и Субъектов Системы в случае выявления инцидентов защиты информации.
2) Участник и Оператор Услуг Платежной Инфраструктуры обеспечивают выполнение этих требований, а также

- установление и применение единых правил реагирования на инциденты;
- создание группы реагирования на инциденты;
- проведение мероприятий по реагированию на каждый обнаруженный инцидент.

3) Оператор обеспечивает учет и доступность для Субъектов Системы информации о выявленных в Системе инцидентах защиты информации и о методиках анализа и реагирования на инциденты защиты информации.

8.14.1. Порядок реагирования и взаимодействия Оператора и Субъектов Системы в случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

1) В случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств

в Системе, не несущего финансовых последствий, но затрагивающего технологические участки, Субъект Системы должен в срок не позднее 24 часов с момента возникновения (выявления) инцидента, а также в течение 24 часов после его устранения, сообщить о нём в доступной форме в службу информационной безопасности Оператора.

В сообщении об инциденте необходимо указать:

- ФИО должностного лица и наименование организации;
- контактные данные;
- место, где произошел инцидент (страну, город, компонент ИТ-инфраструктуры);
- тип инцидента;
- описание инцидента;
- время возникновения инцидента (в случае невозможности установить время возникновения, указывается время выявления).

В случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе несущего финансовые последствия, Субъект Системы должен незамедлительно, не позднее одного часа с момента выявления инцидента, сообщить о нём в доступной форме Оператору.

В сообщении об инциденте необходимо указать:

- ФИО должностного лица и наименование организации;
- контактные данные;
- место, где произошел инцидент (страну, город, компонент ИТ-инфраструктуры);
- тип инцидента;
- описание инцидента;
- время возникновения инцидента (в случае невозможности установить время возникновения, указывается время выявления);
- дату, время и реквизиты сфальсифицированных переводов денежных средств.

Информация направляется в письменном виде (в том числе, может быть доставлена посредством электронной почты, почтовым отправлением, курьерской доставкой).

Ответственное лицо субъекта Системы после получения информации о выявленном инциденте защиты информации 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 защиты информации.

По результатам анализа причин и последствий инцидента защиты информации ответственное лицо по согласованию с непосредственным руководителем в максимально короткие сроки определяет и инициирует первоочередные меры, направленные на локализацию инцидента защиты информации и на минимизацию его последствий.

В процессе проведения мероприятий по устранению последствий инцидента защиты информации ответственным лицом субъекта Платежной Системы должны быть установлены следующие факты:

- дата и время совершения /возникновения инцидента защиты информации;
- тип инцидента защиты информации;
- условия и причина возникновения инцидента защиты информации;
- вид нарушителя, виновного в совершении инцидента защиты информации (внутренний/внешний);
- обстоятельства и мотивы совершения инцидента защиты информации;
- требования по обеспечению защиты информации, вследствие нарушения которых возник инцидент защиты информации;
- последствия инцидента защиты информации;
- действия, необходимые для устранения последствий инцидента защиты информации;
- факт обращения в правоохранительные органы;
- планируемая дата завершения разбирательства по инциденту защиты информации.

По итогам рассмотрения всех сведений об инциденте защиты информации ответственным лицом Субъекта Системы должно быть принято решение о целесообразности применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для нейтрализации последствий инцидентов защиты информации.

По результатам расследования инцидента защиты информации ответственное лицо формирует, согласовывает со всеми участниками разбирательства и подписывает итоговое заключение, включающее установленные факты об инциденте защиты информации, принятые меры по нейтрализации последствий инцидента защиты информации и иные обстоятельства, имеющие отношения к устранению последствий инцидента защиты информации.

В случае выявления в инциденте защиты информации признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, ответственное лицо передает все материалы по инциденту защиты информации в юридическую службу Субъекта Системы для принятия решения о подаче заявления в правоохранительные органы Российской Федерации.

На заключительном этапе устранения последствий инцидента защиты информации ответственное лицо проводит анализ результатов реагирования на инцидент с целью определения достаточности принятых мер.

2) Служба информационной безопасности Оператора незамедлительно, но не позднее одного часа с момента выявления инцидента, инициирует информирование Субъектов Системы в доступной форме по предоставленным ими контактным данным о выявлении инцидента, который оказывает (или может оказать) влияние на работу соответствующего Субъекта. Информация направляется в письменном виде

(в том числе, может быть доставлена посредством электронной почты, почтовым отправлением, курьерской доставкой).

Далее 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 Оператор направляет соответствующее уведомление тому субъекту Системы, в функциональной зоне ответственности которого находится область возникновения инцидента для принятия незамедлительных мер.

3) Субъект Системы, 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.

Для восстановления штатного функционирования объекта информационной инфраструктуры в случае реализации инцидентов защиты информации Субъект Системы 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.

При осуществлении обмена информацией об инцидентах защиты информации Субъекты Системы определяют ответственных лиц для взаимодействия с Оператором и руководствуются пп. 1.5.1 и 1.5.2 Правил.

8.14.2. Предоставление Субъектами Системы Оператору информации для анализа обеспечения в Платежной Системе защиты информации при осуществлении переводов денежных средств.

Субъекты Системы направляют Оператору посредством электронной почты на ежеквартальной основе не позднее пятнадцатого рабочего дня месяца, следующего за отчетным кварталом, в электронном виде отчет. Отчет предоставляется исключительно в отношении инцидентов, выявленных при работе в Системе.

В случае отсутствия за отчетный период инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе, направляется нулевой отчет в целях подтверждения факта информирования Оператора.

8.14.3. Порядок обеспечения Оператором учета и доступности для Субъектов Системы информации о выявленных в Системе инцидентах, связанных с нарушениями требований к

обеспечению защиты информации при осуществлении переводов денежных средств, методиках анализа и реагирования на инциденты.

1) Оператор ведет учет выявленных в Системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в соответствии с внутренними процедурами, разработанными Оператором.
2) Оператор обеспечивает доступность информации о выявленных в Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, путем направления в электронном виде соответствующей информации Субъектам Системы в форме отчета на ежеквартальной основе. В случае отсутствия инцидентов за отчетный период такой отчет не направляется. Кроме того, соответствующая информация предоставляется Субъектам Системы по запросу.
3) Оператор разрабатывает и поддерживает в актуальном состоянии методики анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе, с учетом системного анализа актуальных факторов риска возникновения инцидентов, характера и периодичности возникновения инцидентов.
4) Оператор обеспечивает доступность методик анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, путем направления Участникам и Операторам Услуг Платежной Инфраструктуры методик на регулярной основе по мере их обновления. Направление актуальной версии методик анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Системе, осуществляется не реже одного раза в год.

8.14.4. Порядок восстановления штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации.

1) Оператор обеспечивает надлежащее (штатное) функционирование Системы в соответствии с комплексом мероприятий, предусмотренным Порядком обеспечения БФПС.
2) Субъектами Системы самостоятельно разрабатываются планы обеспечения непрерывности деятельности и восстановления деятельности, в том числе в случае реализации инцидентов защиты информации, в соответствии с требованиями настоящих Правил, и определяется порядок осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий реализации инцидентов защиты информации, а также порядок пересмотра и тестирования данных планов.
3) Оператор и Субъекты Системы информируют друг друга в электронном виде о возобновлении работоспособности после восстановления штатного функционирования инфраструктуры.
4) Оператор определяет следующие требования к мероприятиям по восстановлению штатного функционирования объектов информационной инфраструктуры

Субъектов Системы для обеспечения непрерывности работы Системы в нештатных ситуациях:

- поддержание актуального перечня объектов информационной инфраструктуры, используемых для работы в Системе;
- наличие резервного оборудования, каналов связи, резервных копий программного обеспечения, средств защиты информации, используемых Субъектом для работы в Системе;
- регулярное выполнение процедур резервного копирования операций, осуществленных в Системе, с применением средств защиты информации;
- наличие конкретных восстановительных решений для соответствующего типа объекта информационной инфраструктуры в зависимости от причины возникновения инцидента защиты информации;
- 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.

8.14.6 Мероприятия, проводимые Субъектами Системы в рамках реагирования на инциденты защиты информации в случае их реализации.

Помимо порядка реагирования на инциденты защиты информации при осуществлении переводов денежных средств, установленного выше, Субъекты Системы обеспечивают организационные и технические меры для реализации мероприятий в рамках реагирования на инциденты защиты информации в случае их реализации. Конкретный комплекс мероприятий определяется, разрабатывается и внедряется Субъектами Системы с учетом следующих требований:

1) Субъекты Системы в своих внутренних документах должны определять и поддерживать в актуальном состоянии:

- перечень сотрудников, ответственных за реагирование на инциденты защиты информации в случае их реализации, включая распределение функциональных ролей;
- перечень потенциальных инцидентов защиты информации и сценариев их реализации;
- алгоритм действий (комплекс мероприятий) при реализации инцидента защиты информации с учетом функциональных ролей и типа инцидента защиты информации;
- временной регламент реагирования на инциденты защиты информации с учетом характера и типа инцидента, а также масштаба (включая потенциальный масштаб) негативных последствий инцидента.

2) Для целей реагирования на инциденты защиты информации в случае их реализации Субъекты Системы должны обеспечить наличие и функционирование аппаратных и программных средств, обеспечивающих возможность реализации мероприятий по реагированию на инциденты защиты информации.
3) Перечень мероприятий по реагированию на инциденты защиты информации Субъекта Системы должен включать:

- эскалацию – обеспечение оперативного информирования сотрудников Субъектов Системы, ответственных за мероприятия по реагированию на инцидент защиты информации;
- взаимодействие между Субъектами Системы в соответствии с порядком, установленным настоящими Правилами (п. 8.14.1);
- устранение инцидента защиты информации – комплекс мероприятий, направленных на устранение инцидента защиты информации;
- оценка негативного влияния (причинения ущерба) инцидента защиты информации и выявления негативного влияния (причинения ущерба) в результате инцидента защиты информации третьим лицам (включая определение таких третьих лиц);
- уведомление третьих лиц, определенных в результате оценки негативного влияния (причинения ущерба), о факте инцидента, факте выявления негативного влияния (причиненного ущерба) и необходимых действиях на стороне третьих лиц, направленных на устранение (минимизацию) негативного влияния (ущерба), оказанного (причиненного) в результате инцидента защиты информации (включая, но не ограничиваясь, смену идентификаторов и паролей доступа, замену сертификатов безопасности, обновление программного обеспечения, временный отказ от обмена электронными сообщениями, блокировку пользователей и иные действия);
- восстановление штатного функционирования объектов информационной инфраструктуры;
- анализ инцидента защиты информации;
- разработка комплекса мер по недопущению повторения идентичных (сходных) инцидентов защиты информации;
- иные мероприятия, разработанные и внедренные Субъектом Системы с учетом особенностей его функционирования.

8.15 К определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств предъявляются следующие требования:

1) Документы, составляющие порядок обеспечения защиты информации при осуществлении переводов денежных средств, определяют:

- состав и порядок применения организационных мер защиты информации;
- состав и порядок использования технических средств защиты информации, включая информацию о конфигурации технических средств защиты информации, определяющую параметры их работы;
- порядок регистрации и хранения информации на бумажных носителях и (или) в электронном виде, содержащей подтверждения выполнения порядка применения

организационных мер защиты информации и использования технических средств защиты информации.

2) Оператор устанавливает распределение обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств путем:

- самостоятельного определения Оператором порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- распределения обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств между Оператором и Субъектами Системы.

3) Оператор и Субъекты Системы определяют порядок обеспечения защиты информации при осуществлении переводов денежных средств в рамках распределения обязанностей, установленных Оператором.
4) Для определения порядка обеспечения защиты информации при осуществлении переводов денежных средств Оператор и Субъекты Системы в рамках обязанностей, установленных Оператором, могут использовать:

- положения национальных стандартов по защите информации, стандартов организаций, в том числе стандартов Банка России, рекомендаций в области стандартизации, в том числе рекомендаций Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании;
- результаты анализа рисков при обеспечении защиты информации при осуществлении переводов денежных средств на основе моделей угроз и нарушителей безопасности информации, определенных в национальных стандартах по защите информации, стандартах организаций, в том числе стандартах Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании, или на основе моделей угроз и нарушителей безопасности информации, определенных Оператором и Субъектами Системы.

5) Субъекты Системы обеспечивают выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств.
6) Субъекты Системы обеспечивают назначение лиц, ответственных за выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств.
7) Служба информационной безопасности Субъекта Системы осуществляет контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств, включая:

- контроль (мониторинг) применения организационных мер защиты информации;
- контроль (мониторинг) использования технических средств защиты информации.

8.16 К совершенствованию Оператором и Субъектами Системы защиты информации при осуществлении переводов денежных средств предъявляются следующие требования:

1) Оператор и Субъекты Системы регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных Оператором, в связи с изменениями:

- требований к защите информации, определенных Правилами;
- законодательных актов Российской Федерации;
- нормативных актов Банка России, регулирующих отношения в национальной платежной системе.

2) Субъекты Системы регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях:

- изменения требований к защите информации, определенных 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;
- на основе результатов проведения мероприятий по обнаружению инцидентов защиты информации и реагированию на них;
- изменения целевых показателей величины допустимого остаточного операционного риска.

3) Субъекты Системы обеспечивают формирование и фиксацию решений о необходимости выполнения корректирующих или превентивных действий, в частности пересмотре применяемых мер защиты информации.

4) Принятие решений Субъектом Системы по совершенствованию защиты информации при осуществлении переводов денежных средств согласуется со службой информационной безопасности.

8.17 К оценке выполнения Оператором и Субъектами Системы требований к обеспечению защиты информации при осуществлении переводов денежных средств предъявляются следующие требования:

1) Оператор и Субъекты Системы обеспечивают проведение оценки соответствия уровням защиты информации в соответствии с национальным стандартом РФ ГОСТ Р 57580.2-2018 (далее – ГОСТ Р 57580.2) при осуществлении переводов денежных средств (далее - оценка соответствия) и должны обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018.

2) Оценка соответствия осуществляется Оператором и Субъектами Системы с привлечением сторонних организаций, имеющих лицензию на осуществлении деятельности по технической защите конфиденциальной информации, в соответствии с требованиями законодательства Российской Федерации.

3) Оператор и Субъекты Системы обеспечивают проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России.

4) Порядок проведения оценки соответствия и документирования ее результатов определен в соответствии с законодательством Российской Федерации.

5) Перечень требований к обеспечению защиты информации при осуществлении переводов денежных средств, выполнение которых проверяется при проведении оценки соответствия, определен в соответствии с законодательством Российской Федерации.

6) Сведения о проведении оценки соответствия предоставляются Оператору в виде сводных данных, содержащих:

- наименование Субъекта Системы, проводившего оценку;
- сроки проведения оценки;
- наименование сторонней организации, проводившей оценку, в соответствии с требованиями законодательства Российской Федерации;
- таблицу оценок, входящих в отчет по результатам оценки соответствия ЗИ в соответствии с ГОСТ Р 57580.2.

8.18 К доведению Субъектом Системы до Оператора информации об обеспечении защиты информации при осуществлении переводов денежных средств включаются следующие требования:

1) Оператор устанавливает требования к содержанию, форме и периодичности представления информации, направляемой Субъектами Системы Оператору для целей анализа обеспечения в Системе защиты информации при осуществлении переводов денежных средств.
2) Субъекты Системы обеспечивают выполнение указанных требований.
3) Информация, направляемая Субъектом Системы, Оператору для целей анализа обеспечения в Системе защиты информации при осуществлении переводов денежных средств, включает следующую информацию:

- степень выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- о результатах проведенных оценок соответствия;

- о выявленных угрозах и уязвимостях в обеспечении защиты информации при проведении ежегодного тестирования на проникновение и анализ уязвимостей объектов информационной инфраструктуры в соответствии с требованиями законодательства Российской Федерации;
- о проведении оценки соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже, чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 прикладного программного обеспечения автоматизированных систем и приложений, распространяемых клиентам для совершения действий, непосредственно связанных с осуществлением переводов денежных средств и (или) программного обеспечения, эксплуатируемого на участках, используемых для приема документов, связанных с осуществлением переводов денежных средств, составленных в электронном виде, к исполнению в автоматизированных системах и приложениях с использованием сети Интернет.

8.19 Требования к управлению риском информационной безопасности, а также выявлению и идентификации риска информационной безопасности Субъектом Системы.

Для управления риском информационной безопасности в Системе (далее – риск ИБ) как одним из видов операционного риска, источниками реализации которого являются:

- недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации;
- недостатки прикладного программного обеспечения автоматизированных систем и приложений;
- несоблюдение требований к указанным процессам деятельности Субъектами Системы должна обеспечиваться реализация второго уровня защиты информации для объектов информационной инфраструктуры, определенных национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер", (далее - ГОСТ Р 57580.1-2017) и уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия». (далее - ГОСТ Р 57580.2-2018).

Для реализации требований по управлению риском ИБ, выявлению и идентификации риска ИБ Субъекты Системы в рамках своих полномочий обязаны:

- определить показатели уровня риска ИБ;
- внедрить процессы выявления и идентификации риска ИБ в отношении объектов информационной инфраструктуры;
- на регулярной основе осуществлять мониторинг, выявление и анализ рисков ИБ;
- контролировать уровень риска ИБ.

Субъекты Системы должны выстроить процессы выявления и идентификации риска ИБ в Системе в отношении объектов своей информационной инфраструктуры, 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 Субъектам Системы:

1) определить потенциальные угрозы (риски) в отношении объектов информационной инфраструктуры, используемых Субъектом для работы в Системе;
2) классифицировать риски ИБ в отношении объектов информационной инфраструктуры, используемых Субъектам для работы в Системе;
3) для выявления и идентификации Риска ИБ использовать способы, включающие в себя в том числе, но не ограничиваясь:

- анализ произошедших риск-событий и интервьюирование работников Субъекта Системы, позволяющие установить риски ИБ, оказывающие влияние на работу субъекта в 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 Системе, Субъект должен руководствоваться положениями нормативных актов Банка России, внутренними документами, регламентирующими управление риском ИБ, и требованиями Оператора.

Субъекты Системы самостоятельно обеспечивают выявление Инцидентов ИБ в своей инфраструктуре и реагирование на выявленные инциденты ИБ, включая устранение причин возникновения Инцидентов ИБ, принятие необходимых мер по снижению негативных последствий Инцидентов ИБ, в случае их реализации, и мер по недопущению повторного возникновения Инцидентов ИБ в соответствии с требованиями законодательства и настоящими Правилами.

Субъекты Системы информируют Оператора о выявленных Инцидентах ИБ в порядке и сроки, установленные в настоящих Правилах.

Субъекты Системы участвуют в выявлении и анализе рисков ИБ в Системе и обязаны:

1) проводить анализ и оценку внешних и внутренних факторов, влияющих на информационную безопасность объектов информационной инфраструктуры и бизнес-процессов, в которых участвует Субъект при осуществлении операций в Системе;
2) идентифицировать риски ИБ, которые могут возникнуть при работе в Системе;
3) разработать и поддерживать в актуальном состоянии классификаторы рисков ИБ, риск-событий, причин возникновения риск-событий. При формировании перечня риск-событий учитывать внутренние документы Субъекта Системы, 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 Системе;

4) определить уровни присущего риска ИБ и установить уровень допустимого риска ИБ, выделить значимые риски ИБ, определить вероятность реализации риска ИБ, идентифицированного Субъектом Системы; определить способы управления Риском ИБ и, по необходимости, актуализировать их;
5) вести мониторинг рисков ИБ, в том числе уровней остаточных рисков ИБ, и контролировать их соответствие допустимым уровням Рисков ИБ.

Наряду с указанными требованиями Субъекты Системы должны вести базу инцидентов ИБ; 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 Системы риска ИБ при работе в Системе; обеспечивать выполнение требований по защите информации при осуществлении переводов денежных средств.

Уровень риска ИБ оценивается по четырем показателям:

- числовой итоговой оценке соответствия защиты информации (RГОСТ), проводимой в соответствии с требованиями Положения 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»;
- числовой оценке отдельно по Процессам ЗИ в соответствии с ГОСТ Р 57580.2-2018;
- показателю значимости инцидентов ИБ, определяемом количеством инцидентов и степенью их влияния на Субъект и/или Оператора Платежной Системы;
- показателю количества и объема операций без добровольного согласия клиентов (далее — ПБДС), определяемому как количество и сумма (объем) случаев и (или) попыток переводов денежных средств без добровольного согласия клиента за отчетный период (по данным Субъекта/Оператора и с учетом сведений/обратной связи Банка России по 6828-У).

Таблица 1. Уровень значимости инцидентов ИБ.

| | |
|---|---|
| **Низкий** | Инцидентов ИБ за отчетный период не зафиксировано или выявленные инциденты не оказали влияния на Субъект и Оператора Системы. |
| **Средний** | Произошел один или несколько инцидентов ИБ, повлиявших на Субъекта и Оператора, общая сумма потерь по которым не превышает одного миллиона рублей за отчетный период и/или 1% от уставного капитала Субъекта. |
| **Высокий** | Произошел один или несколько инцидентов ИБ, повлиявших на Субъекта и Оператора. Общая сумма потерь превышает один миллион рублей за отчетный период и/или 1% от уставного капитала Субъекта. |

Таблица 2. Уровень значимости ПБДС (операций без добровольного согласия клиента).

| | |
|---|---|
| **Низкий** | Операции без добровольного согласия клиента отсутствуют. |
| **Средний** | Зафиксированы операции без добровольного согласия клиента, но их количество и сумма не превысили установленных лимитов. |
| **Высокий** | Операции без добровольного согласия клиентов зафиксированы в количестве и суммах, превышающих установленные лимиты. |

Таблица 3. Общий уровень риска.

| | |
|---|---|
| **Низкий** | Итоговый уровень соответствия защиты информации – 4, уровень значимости инцидентов ИБ и уровень значимости ПБДС - низкие. |
| **Средний** | Итоговый уровень соответствия защиты информации – 3, но при этом не менее 4 процессов ЗИ имеют 4 уровень соответствия защиты информации, а остальные процессы ЗИ имеют уровень не ниже 3. Итоговый уровень соответствия защиты информации – 4 и уровни значимости инцидентов ИБ и ПБДС не превышают средний уровень. |
| **Высокий** | Итоговый уровень соответствия защиты информации – 2 и ниже, либо один и более процессов имеют уровень соответствия защиты информации 2 и ниже, при этом итоговый уровень соответствия ЗИ не важен. Уровень значимости инцидентов ИБ и/или ПБДС - высокий. |

При несоблюдении требований к управлению риском информационной безопасности и достижении высокого уровня риска Оператор имеет право существенно (вплоть до 0) снизить лимиты на отправление/выплату переводов денежных средств Участником или проведение операций ОУПИ (ограничение по параметрам операций по осуществлению переводов денежных средств) в рамках Системы до момента соблюдения требований к управлению риском информационной безопасности и повышения уровня защищенности и снижения уровня риска Участника.

Ограничения могут быть сняты по решению Оператора:

- при условии отсутствия инцидентов ИБ и операций без добровольного согласия клиентов в последующие три месяца;
- при условии предоставления документов и информации об устранении причин возникновения инцидентов;
- при условии возмещения Субъектом убытка Оператору Системы.

При достижении среднего уровня риска Оператор имеет право запросить у Участника план повышения уровня защищенности и снижения уровня риска до низкого.

## 9. ПРОТИВОДЕЙСТВИЕ ОСУЩЕСТВЛЕНИЮ ПЕРЕВОДОВ БЕЗ ДОБРОВОЛЬНОГО СОГЛАСИЯ КЛИЕНТОВ

Оператор и Субъекты Системы должны реализовать мероприятия по противодействию осуществлению переводов денежных средств без добровольного согласия клиента, определенных пунктами 4.5 и 4.8 Указания Банка России от 19 августа 2024 года № 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 N 161-ФЗ "О национальной платежной системе", а также о порядке реализации ими мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента».

9.1. Мероприятия по противодействию осуществлению переводов без добровольного согласия клиентов:

9.1.1 Оператор в целях противодействия осуществлению переводов без добровольного согласия клиента:

- создает систему выявления и мониторинга переводов денежных средств без добровольного согласия клиентов;
- назначает и доводит до субъектов Платежной Системы контактные данные подразделения/лица, ответственного за противодействие осуществлению переводов денежных средств без добровольного согласия клиентов;
- определяет порядок противодействия осуществлению переводов денежных средств без добровольного согласия клиента для Участников;
- накапливает и использует для противодействия информацию о способах и технологиях создания переводов денежных средств без добровольного согласия клиента, включая сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Участников и (или) его клиентов, применительно к своей инфраструктуре;
- создаёт систему выявления и мониторинга переводов денежных средств без добровольного согласия клиента, управляемую сводом правил, на основании которых принимается решение о возможности отправки и/или выплаты перевода и которые учитывают особенности поведения клиента, географию его операции, лимиты по операциям и иные критерии;
- использует техническую инфраструктуру (автоматизированную систему) Банка России, информация о которой размещается на официальном сайте Банка России в сети интернет.

9.1.2 Участники обязаны самостоятельно реализовывать мероприятия, направленные на противодействие осуществлению переводов денежных средств без добровольного согласия клиентов, а также незамедлительно (не позднее следующего рабочего дня) информировать

Оператора о выявлении операций, имеющих признаки перевода без добровольного согласия клиента, и о предпринятых Участником действиях в отношении указанных операций. При этом Участник должен:

- выявлять операции по переводу денежных средств, соответствующие признакам осуществления перевода денежных средств без добровольного согласия клиента;
- выявлять операции по переводу денежных средств, совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры Участника;
- выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры Участника и (или) его клиентов, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без добровольного согласия клиента;
- осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Участника и Оператора, других Субъектов Системы;
- осуществлять сбор сведений об обращении плательщика в правоохранительные органы при их наличии;
- рассматривать случаи и (или) попытки осуществления переводов денежных средств без добровольного согласия клиента, вызванные компьютерными атаками, направленные на объекты информационной инфраструктуры Участника и Оператора, других Субъектов Системы;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без добровольного согласия клиента;
- определять в документах, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без добровольного согласия клиента, на основе анализа характера, параметров и объема совершаемых клиентами оператора по переводу денежных средств операций (осуществляемой клиентами деятельности) в соответствии с частью 3.5 статьи 8 Федерального закона N 161-ФЗ;
- реализовывать в отношении клиента - получателя средств, в адрес которого ранее совершались операции по переводу денежных средств без добровольного согласия клиента, в случаях, предусмотренных договором банковского счета, ограничения по параметрам операций по осуществлению переводов денежных средств (переводов электронных денежных средств) с использованием платежных карт, а также ограничения на получение наличных денежных средств в банкоматах за одну операцию и (или) за определенный период времени;
- использовать выявленную Участником информацию о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры оператора по переводу денежных средств и (или) его клиентов, применительно к своей инфраструктуре в целях противодействия осуществлению переводов денежных средств без добровольного согласия клиента.

Мероприятия Участника, направленные на противодействие осуществлению переводов денежных средств без добровольного согласия клиентов, должны включать:

- определение сотрудников (подразделений) Участника, ответственных за реализацию мероприятий, направленных на противодействие осуществлению переводов денежных средств без добровольного согласия клиентов;
- разработку и введение в действие (а также актуализацию) внутренних документов Участника, регламентирующих перечень мероприятий, направленных на противодействие осуществлению переводов денежных средств без добровольного согласия клиентов, и порядок реализации таких мероприятий;
- наличие у Участника достаточных аппаратных и программных средств для обеспечения эффективного противодействия осуществлению переводов денежных средств без добровольного согласия клиентов (включая систему мониторинга операций клиентов);
- своевременное обновление и модернизацию аппаратных и программных средств для обеспечения эффективного противодействия осуществлению переводов денежных средств без добровольного согласия клиентов;
- регулярное обучение сотрудников Участника по вопросам противодействия осуществлению переводов денежных средств без добровольного согласия клиентов;
- проведение мероприятий, направленных на повышение осведомленности клиентов Участника о противодействии осуществлению переводов денежных средств без добровольного согласия клиентов;
- определение порядка приостановки операции клиента в случае выявления Участником операции, совершенной без добровольного согласия клиента, или наличия в операции признаков операции без добровольного согласия клиента;
- определение порядка отказа от совершения операции клиента в случае выявления Участником в операции признаков операции, совершаемой без добровольного согласия клиента.

9.1.3 Оператор по факту получения сообщения от Участника реализует мероприятия, направленные на приостановление такой операции (если она не была приостановлена Участником) до момента получения от Участника сообщения о получении Участником согласия клиента на проведение операции, или до момента истечения срока приостановления такой операции.

9.1.4 ОУПИ при реализации мероприятий по противодействию осуществлению переводов денежных средств без добровольного согласия клиента должны:

- самостоятельно и в полном объеме реализовывать меры по противодействию осуществлению переводов денежных средств без добровольного согласия клиента (Участника) в соответствии с порядком, установленным Оператором в настоящем разделе;
- 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;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без добровольного согласия клиента;
- 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.

Мероприятия, направленные на противодействие осуществлению переводов денежных средств без добровольного согласия клиентов (Участников), реализуемые ОУПИ, должны включать:

- определение сотрудников (подразделений) ОУПИ, ответственных за реализацию мероприятий, направленных на противодействие осуществлению переводов денежных средств без добровольного согласия клиентов;
- разработку и введение в действие (а также актуализацию) внутренних документов ОУПИ, регламентирующих перечень мероприятий, направленных на противодействие осуществлению переводов денежных средств без добровольного согласия клиентов (Участников), и порядок реализации таких мероприятий;
- наличие у ОУПИ достаточных аппаратных и программных средств для обеспечения эффективного противодействия осуществлению переводов денежных средств без добровольного согласия клиентов;
- своевременное обновление и модернизацию аппаратных и программных средств для обеспечения эффективного противодействия осуществлению переводов денежных средств без добровольного согласия клиентов;
- регулярное обучение сотрудников ОУПИ по вопросам противодействия осуществлению переводов денежных средств без добровольного согласия клиентов;
- определение порядка приостановки операции в случае выявления ОУПИ операции, совершенной без добровольного согласия клиента, или наличия в операции признаков операции без добровольного согласия клиента (Участника);
- определение порядка отказа от совершения операции клиента (Участника) в случае выявления ОУПИ в операции признаков операции, совершаемой без добровольного согласия клиента (Участника).

9.1.5 Оператор и Субъекты Системы информируют Банк России о переводах без добровольного согласия клиентов в случаях и в порядке, предусмотренных Указанием Банка России от 19.08.2024 г. №6828-У.

## 10. ПРОТИВОДЕЙСТВИЕ ЛЕГАЛИЗАЦИИ (ОТМЫВАНИЮ) ДОХОДОВ, ПОЛУЧЕННЫХ ПРЕСТУПНЫМ ПУТЁМ, ФИНАНСИРОВАНИЮ ТЕРРОРИЗМА И РАСПРОСТРАНЕНИЯ ОРУЖИЯ МАССОВОГО УНИЧТОЖЕНИЯ

10.1. Оператор и Субъекты Системы осуществляют деятельность, направленную на ПОД/ФТ/ФРОМУ в соответствии с законодательством Российской Федерации и стран деятельности иностранных участников, внутренними документами, разработанными Субъектами Системы.

10.2 Оператор вправе устанавливать дополнительные требования по ПОД/ФТ/ФРОМУ для отдельных Участников в зависимости от способа предоставления Участником доступа своим клиентам к Услугам, включая каналы предоставления Услуг.

10.3 Участники идентифицируют клиентов в соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и законодательством стран деятельности иностранных участников с целью оказания Услуг клиентам, а также с целью оказания Услуг этим же клиентам другими Участниками. Участник передает Оператору идентификационные данные клиента, полученные Участником от клиента при оказании Услуги, для дальнейшего использования этих данных другими Участниками.

10.4 Оператор

- создает и поддерживает базу идентификационных данных (далее БИД), содержащую данные идентифицированных клиентов, полученные Оператором от Участников в рамках идентификации в пользу других Участников;
- предоставляет Участникам данные из БИД для оказания Участниками Услуг клиентам;
- обеспечивает обновление данных в БИД на регулярной основе, не реже 1 раза в год.

10.5 Данные, содержащиеся в БИД, предоставляются Оператором Участникам для

- ускорения и повышения качества обслуживания клиентов;
- предоставления клиентам возможности получения Услуг через системы самообслуживания Участников с подтверждением клиентом идентификационных данных в момент оказания Услуги путем введения клиентом разового кода или пароля.

10.6 При отсутствии сведений об отправителе или получателе перевода денежных средств, наличие которых является обязательным в соответствии с законодательством Российской Федерации и законодательством страны деятельности Иностранного Участника, распоряжение Участника на перевод денежных средств не принимается к исполнению. При

обработке перевода Оператор обеспечивает техническую возможность сопровождения перевода денежных средств всеми необходимыми сведениями.

## 11. СИСТЕМА УПРАВЛЕНИЯ РИСКАМИ

11.1. Цель и область применения.
11.1.1. Система управления рисками (СУР) предназначена для предотвращения и снижения вероятности событий, способных повлиять на бесперебойность функционирования Платёжной Системы (БФПС). Подробный порядок организации и функционирования СУР устанавливается Приложением № 4 к настоящим Правилам.
11.1.2. СУР реализуется с учётом законодательства Российской Федерации и нормативных актов Банка России. Конкретные методики и процедуры приведены в Приложении № 4.

11.2. Организационная модель и распределение ролей.
11.2.1. В Платёжной Системе применяется распределённая модель управления рисками: Оператор, ОУПИ и Участники управляют рисками каждый в пределах своей зоны ответственности.
11.2.2. Оператор устанавливает принципы, требования и показатели СУР, координирует и контролирует исполнение; ОУПИ и Участники внедряют и поддерживают процедуры управления рисками в своих процессах и предоставляют Оператору информацию в установленном порядке (детализация — Приложение № 4, разд. 2–4).

11.3. Принципы управления рисками.
11.3.1. Управление рисками включает идентификацию, оценку, мониторинг и реагирование, включая риски, связанные с привлечением поставщиков услуг (см. Приложение № 4, разд. 2).
11.3.2. Термины «риск-событие», «инцидент» и иные определения применяются в значениях, установленных Приложением № 4.

11.4. Оценки рисков.
11.4.1. Плановые и внеплановые оценки рисков, их триггеры, сроки завершения и состав документации устанавливаются Приложением № 4 (разд. 2).

11.5. Ключевые индикаторы риска и показатели БФПС.
11.5.1. Состав ключевых индикаторов риска (КИР), методики их расчёта и пороговые уровни, а также показатели П1–П5 БФПС и их пороги определены в Приложении № 5. Мониторинг и отчётность по ним выполняются в порядке, установленном Приложением № 4.

11.6. Управление непрерывностью функционирования.
11.6.1. Принципы управления непрерывностью, требования к планам ОНиВД, регламенты выполнения процедур и периоды восстановления оказания услуг устанавливаются Приложением № 4. См. также п. 7.9 настоящих Правил.

11.7. Взаимодействие и обмен информацией.
11.7.1. Порядок, формы, каналы и сроки уведомления Оператора и Субъектов Системы об инцидентах, порядок информирования Банка России, а также состав и сроки представления отчётности по БФПС устанавливаются Приложением № 4.

11.8. Контроль эффективности и пересмотр СУР.
11.8.1. Периодичность оценки СУР, критерии эффективности мероприятий и случаи пересмотра СУР определяются Приложением № 4.

11.9. Документирование и хранение сведений.
11.9.1. Порядок документирования инцидентов и оценок, а также сроки хранения сведений по Системе и инцидентам устанавливаются Приложением № 4.

11.10. Приоритет детализации.
11.10.1. В части процедур, методик, пороговых уровней и регламентов действуют положения Приложения № 4 как неотъемлемой части настоящих Правил.

## 12. КОНТРОЛЬ ЗА СОБЛЮДЕНИЕМ ПРАВИЛ. ОТВЕТСТВЕННОСТЬ. СПОРЫ

12.1. Оператор осуществляет контроль за соблюдением Правил Субъектами Системы следующими способами:

- рассмотрение обращений, поступивших от клиентов и Субъектов Системы в отношении действий (бездействий) Субъектов Системы при оказании услуг;
- сбор и обработка информации о деятельности Субъектов Системы в открытых источниках;
- получение информации о деятельности Субъектов Системы от самого Субъекта и иных Субъектов;
- организация Оператором письменных опросов, рабочих встреч, семинаров, видеоконференций с представителями Участников, операторов услуг платежной инфраструктуры.

12.2. Оператор вправе проводить выборочные проверки соблюдения Правил Субъектами Системы, в том числе с привлечением третьих лиц.

12.3. Субъекты Системы несут ответственность за несоблюдение Правил в соответствии с законодательством Российской Федерации, Правилами и договорами, заключенными в связи с участием в Системе.

12.4. Субъекты Системы несут ответственность за любые действия своих сотрудников, повлекшие ущерб для Субъектов Системы, и обязуются возместить друг другу ущерб, нанесенный в результате таких действий в документально подтвержденном размере.

12.5. В случае неисполнения Субъектом Системы порядка обеспечения БФПС, неоднократного в течение календарного года неисполнения требований Оператора по устранению выявленных нарушений, Оператор вправе принять решение об исключении Субъекта из Системы. Несоблюдение Правил, в том числе порядка обеспечения БФПС, является одним из критериев прекращения участия в Системе, а также критерием прекращения выполнения функций ОУПИ.

12.6. Оператор не несет ответственности за наступление неблагоприятных последствий для третьих лиц, возникших в результате неисполнения Участником или исполнения Участником ненадлежащим образом обязательств, предусмотренных настоящими Правилами, в отношении таких третьих лиц.

12.7. Ответственность Участников за соблюдение Правил наступает с момента присоединения к Правилам.

12.8. Досудебное разрешение споров между Участниками и их клиентами в отношении услуг, оказываемых в рамках Системы, осуществляется в соответствии с процедурами, установленными договорами между Участниками и их клиентами.

12.9. Досудебное разрешение споров между Субъектами Системы 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.

В случае достижения сторонами спора договоренностей о разрешении спора в досудебном порядке стороны фиксируют такую договоренность в письменном виде путем заключения соответствующих соглашений, обмена письмами, подписанием протоколов, иными способами, позволяющими подтвердить достижение сторонами договоренностей о разрешении спора в досудебном порядке.

12.10. В случае недостижения сторонами спора соглашения о разрешении спора в досудебном порядке в течение 60 (шестидесяти) дней с даты направления стороной спора другой стороне спора заявления о споре, а также в случае отсутствия таких переговоров в течение того же периода любая из сторон спора вправе обратиться в суд в соответствии с настоящими Правилами.

12.11. Все споры, разногласия и требования между Участниками и их клиентами, а также между Оператором и клиентами Участников, связанные с оказанием Участниками услуг, при недостижении сторонами договоренности в досудебном порядке подлежат разрешению в судах Российской Федерации в соответствии с их подсудностью.

12.12. Все споры, разногласия или требования между Оператором и Субъектами Системы, между Субъектами Системы при недостижении договоренности в досудебном порядке подлежат разрешению в Арбитражном суде г. Москвы. На основании дополнительного соглашения между собой Субъекты Системы могут передать спор на рассмотрение третейского суда.

12.13. Контроль за соблюдением порядка обеспечения БФПС

12.13.1. Оператор осуществляет контроль за соблюдением Субъектами Системы порядка обеспечения БФПС способами, установленными в Приложении №4 к настоящим Правилам.

12.13.2. При выявлении нарушений порядка обеспечения БФПС Оператор вправе применить к нарушителю санкции, предусмотренные настоящими Правилами.

## 13. ВЗАИМОДЕЙСТВИЕ С ДРУГИМИ ПЛАТЕЖНЫМИ СИСТЕМАМИ

Платежная система “Система банковской кооперации” не взаимодействует с другими платежными системами.

## 14. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Все вопросы, не урегулированные в настоящих Правилах, регулируются Законодательством, договорами между Субъектами Системы и внутренними документами Оператора.

Если в результате изменения Законодательства отдельные статьи Правил вступают в противоречие с ним, эти статьи утрачивают силу и до момента внесения изменений в Правила, Участники руководствуются Законодательством.

Приложение № 1
к Правилам Платежной Системы
«Форма заявления на участие в Платежной Системе»

Исх. № _____

Дата: _____ 202__ г.

Оператору Платежной Системы

от_____

_____

_____

Заявление на участие в Платежной Системе

Настоящим_____
(наименование организации)

в лице_____,
(ФИО и должность уполномоченного представителя Заявителя)

действующего(ей) на основании_____
(наименование документа, уполномочивающего представителя Заявителя на подачу данного заявления от имени Заявителя)
(далее «Заявитель»), направляет оператору Платежной Системы ООО «Оператор банковской кооперации» (далее «Оператор») настоящее заявление на участие в Платежной Системе в качестве Участника.

1. В целях рассмотрения Оператором настоящего заявления и принятия решения о возможности участия Заявителя в Платежной Системе настоящим Заявитель направляет в адрес Оператора документы согласно перечню, указанному в пункте 6 ниже. Заявитель подтверждает полноту и достоверность данных, содержащихся в прилагаемых документах.
2. Заявитель подтверждает, что ознакомился с Правилами Платежной Системы, размещенными на официальном сайте Оператора, действующими на дату настоящего заявления, и настоящим заявляет о своем согласии с указанными Правилами.
3. Заявитель понимает и соглашается с тем, что факт получения Оператором настоящего Заявления не влечет автоматического присоединения Заявителя к Платежной Системе и не налагает на Оператора каких-либо обязательств направить Заявителю договор об участии в Платежной Системе в качестве Участника.
4. Заявитель настоящим обязуется обеспечить конфиденциальность информации, которую Оператор может направить Заявителю в договоре участия или предоставить иным образом. Заявитель обязуется не разглашать такую информацию третьим лицам. Заявитель понимает, что разглашение информации, предоставленной Заявителю Оператором после получения настоящего Заявления, является основанием для отзыва договора участия Оператором и взыскания с Заявителя

любых убытков и ущерба, причиненных Оператору в результате разглашения Заявителем соответствующей информации.

5. По всем вопросам, связанным с настоящим заявлением, просим обращаться к нашему ответственному сотруднику

_____

(ФИО и должность ответственного сотрудника)

по телефону или email _____.

6. Настоящее заявление составлено в одном экземпляре с приложением следующих документов:

    1. Копия свидетельства о государственной регистрации юридического лица.
    2. Копия свидетельства о постановке на учет в налоговом органе.
    3. Копия лицензии на совершение банковских операций.
    4. Копия Устава, копии зарегистрированных дополнений и изменений к ним.
    5. Копия выписки из ЕГРЮЛ (уполномоченного государственного органа регистрации юридических лиц);
    6. Копии документов, подтверждающих избрание и назначение на должность единоличного исполнительного органа организации.
    7. Копии документов, необходимых для определения срока полномочий единоличного исполнительного органа организации;
    8. Копия документа, подтверждающего полномочия лица, подписывающего заявление и иные документы от имени организации, присоединяющейся к Правилам платежной системы «Система банковской кооперации» (протокол, решение, приказ о назначении руководителя, доверенность, т.д.);

Всего _____ листов.

От имени Заявителя:

_____

(должность)

_____

(ФИО)

_____

(подпись)

Приложение № 2
к Правилам Платежной Системы

# УСЛОВИЯ ОКАЗАНИЯ УСЛУГИ ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ

На территории Российской Федерации услуга по переводу денежных средств (далее «Услуга») предоставляется российскими банками-участниками платежной системы «Система банковской кооперации» (далее ПС «СБК») в соответствии с настоящими Условиями оказания Услуги (далее «Условия оказания Услуги»). За пределами Российской Федерации Услуги предоставляются иностранными банками-участниками.

При осуществлении перевода денежных средств отправитель перевода денежных средств заключает договор с банком-участником ПС «СБК» в форме поручения на осуществление перевода денежных средств в соответствии с настоящими Условиями оказания Услуги, которые являются неотъемлемой частью договора между банком и отправителем перевода денежных средств.

Отправляя (получая) перевод денежных средств, отправитель (получатель) денежных средств выражает свое согласие с настоящими Условиями оказания Услуги.

1. Определения.

**Банк** – участник ПС «СБК».

**Документ, удостоверяющий личность** – документ, удостоверяющий личность отправителя (получателя) перевода денежных средств в соответствии с законодательством страны отправления (назначения) перевода денежных средств.

**Идентификация** – совокупность мероприятий по установлению сведений о клиенте и подтверждению достоверности этих сведений с использованием оригиналов документов и (или) надлежащим образом заверенных копий и (или) государственных и иных информационных систем.

**Контрольный Номер Перевода (КНП)** – цифровой код, присваиваемый процессингом ПС «СБК» переводу и являющийся одним из реквизитов перевода.

**Оператор Платежной Системы (Оператор)** – ООО «Оператор банковской кооперации», зарегистрированное Банком России в реестре операторов платежных систем под номером 46 от 23.01.2018 и являющееся оператором платежной системы «Система банковской кооперации».

**Плата за перевод** – плата, взимаемая с клиента за оказание Услуги.

**Поручение на осуществление выплаты денежных средств** – поручение, передаваемое получателем банку через мобильное приложение платежной системы или при личном посещении отделения банка. Содержит обязательные реквизиты перевода денежных средств и является основанием для выплаты перевода денежных средств получателю.

**Поручение на осуществление перевода денежных средств** – поручение на осуществление перевода денежных средств в пользу физического или юридического лица

в рамках Платежной Системы, передаваемое отправителем Банку (в том числе в электронном виде) и являющееся договором между отправителем и Банком.

**Мобильное приложение платежной системы** – программное обеспечение, принадлежащее Оператору, и обеспечивающее отправителю/получателю доступ к услугам Банка для отправки и получения переводов денежных средств.

2. Отправка перевода денежных средств.

2.1. При отправлении перевода денежных средств через Платежную Систему отправитель должен:

- пройти идентификацию;
- предоставить Банку распоряжение с указанием суммы перевода в рублях, номера телефона и страны (если перевод трансграничный) получателя;
- подтвердить перевод.

2.2. Перевод денежных средств, осуществляемый в рамках Услуги, не должен быть связан с осуществлением отправителем предпринимательской деятельности, инвестиционной деятельности или приобретением отправителем прав на недвижимое имущество.

2.3. Идентификация. Банк осуществляет идентификацию (упрощенную идентификацию) отправителя в соответствии с требованиями законодательства Российской Федерации в области противодействия отмыванию доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (далее «ПОД/ФТ/ФРОМУ»).

2.4. Плата за отправку перевода взимается Банком. Плата за выплату перевода – выдачу наличными или зачисление на счет - не взимается.

2.5. Конвертация. Перевод денежных средств из Российской Федерации отправляется в российских рублях (с учетом применимых ограничений, установленных законодательством Российской Федерации). За пределами Российской Федерации такой перевод денежных средств может быть выплачен в валюте отправления или в иной валюте с учетом применимых законодательных ограничений страны назначения перевода денежных средств и наличия соответствующей валюты в пункте выплаты перевода денежных средств. Отправитель имеет право указать в качестве валюты выплаты перевода денежных средств в стране назначения валюту, отличную от валюты отправления перевода денежных средств (с учетом возможностей, предоставляемых в стране назначения перевода денежных средств). При этом курс, по которому валюта отправления пересчитывается в валюту выплаты перевода денежных средств, выбранную отправителем, а также сумма в валюте выплаты сообщаются отправителю перевода денежных средств при отправлении соответствующего перевода.

2.6. Ограничения по сумме перевода. Максимальная сумма одного перевода денежных средств, отправляемого с использованием Платежной Системы, не может превышать эквивалента 5000 долларов США в российских рублях по курсу Банка России на день отправления перевода денежных средств.

Суммы лимитов могут корректироваться Оператором и/или Банками (по согласованию с Оператором) в сторону уменьшения с учетом требований законодательства Российской Федерации, включая любые временные правила и ограничения, устанавливаемые Президентом Российской Федерации, Правительством Российской Федерации или Банком

России. Оператором Платежной Системы или Банками по договоренности с Оператором, могут быть установлены дополнительные ограничения в пределах сумм, указанных выше, с учетом особенностей способов предоставления Банком доступа своим клиентом к Услуге.

2.7. Информация об условиях выплаты. Перед отправлением перевода денежных средств отправитель обязан ознакомиться с информацией об условиях выплаты перевода денежных средств в стране назначения перевода денежных средств, в том числе с применимыми ограничениями и лимитами на выплату денежных средств. Эта информация может быть получена в мобильном приложении платежной системы. Отправляя перевод денежных средств, отправитель подтверждает, что он/она ознакомлен/а с условиями выплаты перевода денежных средств в стране назначения перевода денежных средств, в том числе с применимыми ограничениями и лимитами на выплату денежных средств.

2.8. Информация, предоставляемая отправителем получателю. После отправления перевода денежных средств отправитель должен сообщить получателю реквизиты перевода денежных средств, необходимые для получения перевода денежных средств с учетом условий выплаты и применимых ограничений, действующих в стране назначения перевода денежных средств. Обычно предоставляются следующие реквизиты:

- полные имя, отчество (при наличии) и фамилия отправителя;
- страна отправления;
- сумма перевода;
- КНП.

2.9. Предупреждение о мошенничестве. В целях избежания выплаты денежных средств лицу, не являющемуся получателем перевода, отправитель ни при каких обстоятельствах не должен сообщать какие-либо реквизиты перевода денежных средств (включая, но не ограничиваясь, КНП) третьим лицам, за исключением получателя. Отправитель обязуется не использовать Услугу в качестве обеспечения оплаты товаров и услуг, так как любая передача информации о переводе третьим лицам увеличивает риск мошенничества и может привести к утрате отправителем денежных средств. Ни при каких обстоятельствах Банк или Оператор не будут нести ответственность перед отправителем в случае сообщения отправителем какой-либо информации о переводе денежных средств кому-либо, за исключением получателя.

3. Выплата перевода денежных средств.

3.1. Для получения перевода денежных средств наличными получатель должен лично пройти идентификацию и дать Банку поручение с указанием следующей информации:

- сумма к выплате;
- КНП.

Поручение может содержать дополнительную информацию и реквизиты, обусловленные конкретным видом Услуги и/или требованиями законодательства.
Поручение подписывается получателем собственноручно.

3.2. Для получения перевода денежных средств безналично получатель должен воспользоваться мобильным приложением платежной системы, пройти идентификацию, дать и подтвердить поручение с указанием банковского счета или карты для выплаты перевода.

3.3. Получая перевод денежных средств, получатель подтверждает, что перевод денежных средств не связан с осуществлением предпринимательской деятельности, инвестиционной деятельности, приобретением прав на недвижимое имущество.

3.4. Идентификация. Банк осуществляет идентификацию (упрощенную идентификацию) получателя в соответствии с требованиями законодательства Российской Федерации в области противодействия отмыванию доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения (далее «ПОД/ФТ/ФРОМУ»). Требования к идентификации клиентов в других странах устанавливаются в соответствии с нормами местного и международного законодательства.

3.5. Сроки оказания Услуги. Перевод денежных средств, направляемый в пользу физического лица, может быть выдан получателю через несколько минут после присвоения такому переводу денежных средств КНП. Денежный перевод, невостребованный получателем, сохраняется в течение 3 дней, после чего возвращается отправителю.

4. Внесение изменений в отправленный перевод и аннулирование отправленного перевода отправителем возможны, если перевод не выплачен и не находится в процессе выплаты. Плата за перевод, возвращённый отправителю вследствие не востребования получателем, не возвращается.

5. Защита персональных данных.

Отправитель и получатель предоставляют свое согласие Банку, Оператору или любому оператору платежной инфраструктуры ПС «СБК» (в том числе за пределами РФ) на обработку (включая, без ограничения, сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (включая трансграничную передачу), обезличивание, блокирование, удаление, уничтожение) своих персональных данных для целей предоставления им Услуги и соблюдения требований местного, зарубежного и международного законодательства.

Одновременно отправитель и получатель перевода денежных средств соглашаются на обработку своих персональных данных Оператором для целей анализа, обработки статистических данных и улучшения качества обслуживания. Право на распространение персональных данных субъектом не предоставляется.

В случае отказа отправителя или получателя от предоставления согласия на обработку персональных данных кому-либо из лиц, указанных выше, Услуга не может быть оказана.

Субъект персональных данных имеет право отозвать свое согласие на обработку персональных данных в любое время путем направления письменного уведомления Оператору об отзыве своего согласия на обработку персональных данных через мобильное приложение платежной системы. В течение 30 (тридцати) дней после получения такого уведомления все лица, указанные выше, прекратят обработку персональных данных субъекта персональных данных.

Банк, Оператор или любой оператор платежной инфраструктуры ПС «СБК» (в том числе за пределами РФ) имеют право продолжить обработку персональных данных субъекта персональных данных после получения от него уведомления об отзыве согласия на обработку персональных данных:

- до момента завершения оказания Услуги;
- если продолжение обработки персональных данных обусловлено требованиями применимого законодательства (в таком случае обработка персональных данных

осуществляется в пределах, необходимых для выполнения требований законодательства).

Любое согласие действует в течение неограниченного периода времени, за исключением случаев отзыва согласия субъектом персональных данных.

6. Прочие положения.

6.1. Настоящие Условия оказания Услуги вступают в силу со дня вступления в силу Правил Платежной Системы и действуют вплоть до отмены или изменения Условий оказания Услуги Оператором.

6.2. Отсутствие правоотношений. Настоящие Условия оказания Услуги не являются публичной офертой Оператора. Оператор не вступает в правоотношения по предоставлению Услуги с отправителем или получателем Услуги.

6.3. Независимость положений. Любое положение настоящих Условий оказания Услуги является самостоятельным положением. В случае неисполнимости какого-либо положения настоящих Условий оказания Услуги все иные положения продолжат действовать и должны быть исполнены в полном объеме. Признание какого-либо положения настоящих Условий оказания Услуги недействительным или незаконным в порядке, предусмотренном законодательством, не влечет недействительности остальных положений и не прекращает их действия. В случае признания в установленном законом порядке отдельных положений настоящих Условий оказания Услуги недействительными или незаконными Оператор изменит или удалит соответствующие недействительные или незаконные положения.

6.4. Ограничение ответственности. Банк, Оператор или любой оператор платежной инфраструктуры ПС «СБК» не гарантируют доставку или качество любых товаров или услуг, оплаченных посредством Услуги. Реквизиты и любая иная информация о переводе денежных средств являются конфиденциальной информацией и не должны сообщаться отправителем третьим лицам, за исключением получателя. Отправитель не должен отправлять перевод денежных средств лицу, которого он не знает. Отправитель обязуется не использовать Услугу в качестве обеспечения оплаты товаров и услуг, в том числе при приобретении товаров и услуг в сети Интернет, так как любая передача информации о переводе третьим лицам
увеличивает риск мошенничества и может привести к утрате денежных средств. Ни при каких обстоятельствах Банк, Оператор или любой оператор платежной инфраструктуры ПС «СБК» (в том числе за пределами Российской Федерации) не несут ответственность за утрату отправителем денежных средств, если отправитель сообщает какие-либо реквизиты перевода денежных средств третьим лицам, за исключением получателя.

6.5. Порядок изменения Условий оказания Услуги. Оператор имеет право вносить изменения в настоящие Условия оказания Услуги в соответствии правилами внесения изменений в Правила.

Приложение № 3
к Правилам Платежной Системы

# ТАРИФЫ

## 1. ТЕРМИНЫ

**Тариф** – плата, взимаемая с клиента Участником по тарифам, установленным Участником с учетом ограничений, установленных Оператором.

**Системное межбанковское вознаграждение** – плата Участника Участнику за предоставление Клиенту услуг Системы.

**Системный тариф Оператора** – плата, взимаемая Оператором с Участника за предоставление услуг платежной инфраструктуры.

## 2. СИСТЕМНЫЕ ТАРИФЫ И ВОЗНАГРАЖДЕНИЯ

2.1. Оператор взимает с российских Участников плату в размере 10000 рублей в год за предоставление услуг платежно-клирингового центра. Плата вносится ежегодно не позднее 1 марта года, следующего за полным годом оказания услуг.

2.2. Межбанковские вознаграждения по трансграничным переводам устанавливаются с учетом особенностей деятельности иностранных участников и указываются в договорах участия.

2.3. Межбанковские вознаграждения по операциям между российскими Участниками устанавливаются и вводятся в действие в соответствие с нормами 161-ФЗ «О национальной платежной системе».

## 3. ТАРИФЫ.

3.1. С клиентов - получателей трансграничных переводов комиссия за выплату переводов не взимается.

Приложение № 4
к Правилам Платежной Системы

Порядок обеспечения БФПС в ПС «СБК»

Общие положения.

Настоящий Порядок разработан с учётом требований Положения Банка России от 03.10.2017 № 607-П «О требованиях к обеспечению бесперебойности функционирования платежной системы», а также иных нормативных актов Банка России, регулирующих деятельность операторов платёжных систем и операторов услуг платёжной инфраструктуры.

1. ООО «Оператор банковской кооперации» (далее - «Оператор»), являющееся оператором Системы «Система банковской кооперации» (далее «Система») и совмещающее функции Оператора с функциями платежно-клирингового центра, обеспечивает бесперебойность функционирования Системы (далее «БФПС») путем осуществления скоординированной с Участниками деятельности:

- по организации системы управления рисками (далее «СУР»), оценке и управлению рисками в Системе;
- по выявлению оказания услуг платежной инфраструктуры (далее «УПИ»), не соответствующего требованиям к оказанию услуг, обеспечению функционирования Системы в случае нарушения оказания УПИ, соответствующего требованиям к оказанию услуг, и восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг, включая восстановление оказания УПИ в случае приостановления их оказания в течение периодов времени, установленных Оператором в настоящем Порядке.

В целях обеспечения требований к БФПС, установленных нормативными документами Банка России, Оператор определяет порядок обеспечения и соблюдения Субъектами Системы БФПС (далее «Порядок»), который включает:
- управление рисками в Системе;
- управление непрерывностью функционирования Системы;
- организацию взаимодействия Субъектов Системы по обеспечению БФПС;
- контроль за соблюдением настоящего Порядка.

Оператор в настоящем Порядке обеспечивает управление рисками с учетом следующих требований:

- Оператор организует СУР в Системе с учетом организационной модели управления рисками в Системе, выбранной в соответствии с требованиями части 2 статьи 28 Федерального закона №161-ФЗ;
- Оператор применяет способы управления рисками в Системе, предусмотренные п. 5 статьи 28 Федерального закона №161-ФЗ (далее «Способы управления рисками»);
- Оператор определяет ключевые индикаторы риска (далее «КИР»), устанавливает и пересматривает с использованием результатов оценки рисков в Системе пороговые уровни КИР;

- Оператор проводит оценку СУР в Системе, в том числе используемых методов оценки рисков в Системе, результатов применения способов управления рисками в Системе, не реже одного раза в три года и документально оформляет результаты указанной оценки. Оценка СУР проводится внепланово в случаях, установленных пунктом 2.6 Положения Банка России № 607-П от 03.10.2017 "О требованиях к обеспечению бесперебойности функционирования платежной системы", в частности при внесении существенных изменений в бизнес-процессы Системы.
- Оператор проводит плановую оценку рисков в Системе, а также внеплановые оценки рисков в Системе с использованием методик анализа рисков в Системе и составлением профилей рисков;
- Оператор проводит внеплановую оценку всех рисков в Системе при внесении изменений в один или несколько бизнес-процессов (перечислены в Приложении 5.4), в рамках которых обеспечивается оказание услуг платежной инфраструктуры. Проведение внеплановой оценки всех рисков в Системе должно быть завершено не позднее истечения шести месяцев со дня внесения указанных изменений;
- Оператор проводит внеплановую оценку рисков (отдельного риска) в Системе:
    - при возникновении события, реализация которого привела к приостановлению (прекращению) оказания УПИ и описание которого в профиле рисков не предусмотрено, либо негативные последствия от его реализации превышают негативные последствия, предусмотренные для этого события в профиле риска;
    - 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 Системе;
    - при выявлении значимого риска в Системе, для которого уровень присущего риска до применения Способов управления рисками в Системе может превысить или превысил уровень допустимого риска;

Проведение внеплановой оценки отдельных рисков (отдельного риска) в Системе должно быть завершено не позднее истечения четырех месяцев:

- со дня возникновения события, реализация которого привела к приостановлению (прекращению) оказания УПИ;
- со дня возникновения факта приближения фактического уровня риска к уровню допустимого риска;
- со дня выявления значимого риска в Системе.

Плановая оценка всех рисков в Системе проводится Оператором не реже одного раза в год с учетом сведений о событиях, которые произошли в Системе со дня завершения предыдущей плановой или внеплановой оценки всех рисков в Системе и привели к приостановлению (прекращению) оказания УПИ.

- Оператор управляет непрерывностью функционирования Системы с учетом следующих требований:
    - Оператор организует деятельность по управлению непрерывностью функционирования Системы и устанавливает права и обязанности Субъектов Системы по управлению непрерывностью функционирования Системы в зависимости от организационной модели управления рисками в Системе;

- Оператор организует сбор и обработку сведений, используемых для расчета КИР;
- Оператор обеспечивает сбор, в том числе от операторов услуг платежной инфраструктуры, обработку и хранение информации по Системе и сведений об инцидентах в Системе не менее пяти лет с даты получения. Под информацией по Системе понимаются сведения о функционировании платежной системы, включая данные о переводах денежных средств, показатели качества функционирования операционных и технологических средств, информационные системы, а также иная информация, необходимая для обеспечения бесперебойности функционирования платежной системы. Влияние инцидента на БФПС определяется с учетом требований, предусмотренных подпунктом 2.3.5 пункта 2.3 Положения Банка России от 03.10.2017 № 607-П «О требованиях к обеспечению бесперебойности функционирования платежной системы»;
- Оператор организует деятельность по разработке регламентов выполнения процедур и контролирует их соблюдение;
- Оператор проводит оценку влияния на БФПС каждого произошедшего в Системе инцидента в срок не позднее рабочего дня, следующего за днем возникновения (выявления) инцидента, а также в срок не позднее окончания рабочего дня, следующего за днем устранения последствий инцидента (восстановления оказания УПИ, соответствующих требованиям к оказанию услуг), и оценку влияния на БФПС всех инцидентов, произошедших в Системе за календарный месяц, в течение пяти рабочих дней после дня окончания календарного месяца, в котором возникли инциденты;
- Оператор устанавливает в настоящем Порядке периоды времени, в течение которых должно быть восстановлено оказание УПИ в случае приостановления их оказания и восстановление оказания УПИ, соответствующее требованиям к оказанию услуг, в случае нарушения указанных требований;
- Оператор устанавливает уровни оказания УПИ, характеризующие качество функционирования операционных и технологических средств платежной инфраструктуры (Приложение 5.3 к настоящему Порядку);
- Оператор разрабатывает и включает в План действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности ООО «Оператор банковской кооперации» в случае возникновения нестандартных и чрезвычайных ситуаций (далее «План ОНиВД») мероприятия, направленные на управление непрерывностью функционирования Системы в случае возникновения инцидентов, связанных с приостановлением оказания УПИ или нарушением установленных уровней оказания УПИ; При совмещении в Системе функций оператора платежной системы и платежно-клирингового центра в План ОНиВД включаются:
- переход Оператора на оказание УПИ через резервный комплекс программных и технических средств;
- переход Оператора на использование резервных сервисов поставщиков услуг;
- мероприятия, осуществляемые в случае неработоспособности систем и сервисов поставщиков услуг, нарушение предоставления которых способно привести к приостановлению оказания УПИ;

- Оператор анализирует эффективность мероприятий по восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг и использует полученные результаты при управлении рисками в Системе;

- Оператор разрабатывает, проверяет (тестирует) и пересматривает План ОНиВД с периодичностью не реже одного раза в два года;
- Оператор обеспечивает оказание УПИ при возникновении инцидентов, а также организует в течение установленных периодов времени восстановление оказания услуг Операторами УПИ в случае приостановления их оказания и восстановление оказания УПИ, соответствующего требованиям к оказанию услуг, в случае нарушения указанных требований.

Оператор организует взаимодействие Субъектов Системы по обеспечению БФПС с учетом следующих требований:

- Оператор устанавливает организационную модель управления рисками в Системе и определяет порядок взаимодействия Субъектов Системы при реализации мероприятий, предусмотренных главами 2 и 3 настоящего Порядка;
- Оператор информирует Банк России и Участников о случаях и причинах приостановления (прекращения) оказания УПИ;
- Оператор проверяет соблюдение Операторами УПИ и Участниками Порядка обеспечения БФПС.
- Оператор устанавливает время устранения инцидента, восстановления УПИ, в том числе в соответствии с требованиям к оказанию услуг.
- Время восстановления услуг при приостановлении их оказания – 6 часов с момента нарушения УПИ;
- Время восстановления в соответствии с требованиями к оказанию услуг – 72 часа с момента нарушения требований к оказанию услуг.

## 2. Управление рисками в Системе

2.1. СУР в Системе включает в себя комплекс мер, установленных настоящим Порядком, направленных на предотвращение или снижение вероятности возникновения неблагоприятных последствий финансового и нефинансового характера, влияющих на БФПС.

2.2. Обеспечение БФПС означает способность поддержания надлежащего функционирования Системы в соответствии с законодательством, Правилами Системы (далее «Правила»), договорами с Субъектами Системы.

2.3. Под риском понимается возможность (вероятность) отклонения от ожидаемого результата в деятельности Системы, причинение ущерба Субъектам Системы и (или) ухудшения ликвидности вследствие наступления неблагоприятных событий, связанных с внутренними или внешними факторами.

2.4. Под риск-событием понимается событие, реализация которого может привести к возникновению инцидента.

2.5. Инцидент – это риск-событие, которому присвоен соответствующий уровень воздействия на деятельность Системы по критериям существенности (значимости) риск-событий. Инцидент может привести к нарушению оказания УПИ в соответствии с требованиями к оказанию услуг и повлиять на БФПС.

2.6. Организационная модель управления рисками.

В Платёжной Системе применяется распределённая модель управления рисками. Оператор, Операторы услуг платёжной инфраструктуры (ОУПИ) и Участники управляют рисками каждый в пределах своей зоны ответственности.

Оператор: устанавливает принципы, требования и показатели СУР, допустимые уровни риска, состав КИР и показатели П1–П5, методики их расчёта и мониторинга; организует и координирует процессы СУР в Системе; проводит плановые и внеплановые оценки рисков, стресс-тестирование значимых рисков; формирует и актуализирует профили рисков; организует управление непрерывностью функционирования, сбор и хранение сведений, обмен информацией и эскалацию; контролирует выполнение требований СУР Субъектами Системы и принимает решения по применению способов управления рисками.

Операторы услуг платёжной инфраструктуры (ОУПИ): управляют рисками, связанными с оказанием ими операционных, клиринговых и расчётных услуг; поддерживают непрерывность оказания УПИ; исполняют регламенты и пороговые уровни, установленные Оператором; обеспечивают регистрацию инцидентов, подготовку отчётности и своевременное информирование Оператора; включают в планы ОНиВД меры по переходу на резервные мощности и взаимодействию при инцидентах.

Участники: управляют рисками в своих процессах, влияющих на Платёжную Систему; обеспечивают защиту информации и непрерывность; регистрируют и уведомляют об инцидентах; предоставляют данные для СУР в сроки и по формам, установленным настоящим Порядком и Правилами.

Границы ответственности, порядок взаимодействия, обмена информацией и эскалации определены главами 2–6 настоящего Порядка.

2.7. Обязанности Субъектов Системы по управлению рисками.

2.7.1. Оператор обязан:

- определить организационную структуру СУР Оператора;
- обеспечить контроль выполнения Операторами УПИ и Участниками Системы требований СУР;
- с учетом выбранной модели управления рисками в Системе определить методики анализа рисков в Системе, включая классификацию рисков, методы их выявления и оценки, определение присущих и остаточных уровней рисков и установку допустимых уровней рисков, а также Способов управления рисками с целью снижения их уровней;
- проводить стресс-тестирование значимых рисков Системы;
- осуществлять мероприятия по составлению профиля рисков Системы;
- выявлять инциденты на основании положений настоящего Порядка, определять уровни их влияния на деятельность, в том числе нарушение УПИ в соответствии с требованиями к оказанию услуг и влияние на БФПС;
- определять КИР, устанавливать их пороговые уровни, а также разрабатывать методы их мониторинга и оценки;
- выполнять расчет и мониторинг значений КИР (в том числе сравнение фактических значений с пороговыми значениями КИР);
- вносить изменения в СУР;
- определять порядок обмена информацией между Субъектами Системы, в том числе о риск-событиях (инцидентах) в Системе;

- определять порядок действий Субъектов Системы при возникновении спорных, нестандартных и чрезвычайных ситуаций;
- определять операционные и технологические требования к программно-аппаратным комплексам Системы и процедурам предоставления услуг Системы и контролировать их исполнение;
- определять требования к порядку оценки качества и надежности функционирования информационных систем, операционных и технологических средств Субъектов Системы;
- определять требования по обеспечению защиты информации в Системе и контролировать их выполнение.

2.7.2. Участники обязаны сообщать Оператору:
- о неисполнении или ненадлежащем исполнении своих обязательств;
- о наличии претензий, предписаний от Банка России в отношении их деятельности в качестве Участников;
- о получении претензий от клиентов в отношении их деятельности в качестве Участников;
- о возникновении инцидентов, касающихся переводов денежных средств, осуществленных Участником в рамках Системы, в соответствии с п.3.3 настоящего Порядка.

Порядок обмена информацией, необходимой для управления рисками.

1) Триггеры обмена:
1. выявление риск-события или инцидента, потенциально влияющего на БФПС;
2. приближение фактического уровня риска к допустимому уровню по данным мониторинга КИР;
3. нарушение уровней оказания УПИ или приостановление оказания УПИ;
4. выявление значимого риска (по профилю).

2) Сроки передачи сведений:
1. при приостановлении/риске приостановления оказания УПИ либо нарушении уровней УПИ — в течение 1 часа с момента выявления;
2. при инцидентах ИБ без влияния на УПИ — в течение 24 часов;
3. ежемесячно — до 5-го рабочего дня следующего месяца — агрегированные значения КИР и оценка влияния инцидентов;
4. по запросу Оператора — в срок, указанный в запросе.

3) Каналы и формат: защищённая почта/СЭДО; установленная форма уведомления/отчёта (минимум: дата/время, описание, затронутые процессы/сервисы, влияние на БФПС/УПИ, КИР/показатели, принятые меры, прогноз восстановления).

4) Роли и эскалация: у Субъекта — ответственный за СУР; у Оператора — ответственное подразделение СУР. Оператор консолидирует сведения и доводит их до органов управления Оператора ПС (см. Правила) и, при необходимости, до Субъектов.

5) Учёт и хранение: единый журнал уведомлений с хранением не менее 5 лет; периодические учения/тесты порядка обмена не реже 1 раза в год.

2.7.3. Обязанности Операторов УПИ.

Все Операторы УПИ (Операционный центр и Расчётные центры) обязаны включать в планы ОНиВД:

- регламенты оперативного информирования Оператора и участников о ходе/результатах переключения и восстановления.
- мероприятия на случай неработоспособности систем и сервисов поставщиков услуг, нарушение предоставления которых способно привести к приостановлению оказания УПИ и/или к нарушению установленных уровней оказания УПИ;
- мероприятия по переходу на резервный комплекс программных и (или) технических средств в случае приостановления оказания УПИ и/или нарушения установленных уровней оказания УПИ;

2.8. Анализ рисков в Системе осуществляется с применением методов, предусмотренных национальным стандартом Российской Федерации ГОСТ Р 58771-2019 «Менеджмент Риска. Технологии оценки риска», утвержденным и введенным 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»).

2.9. Методика анализа рисков в Системе включает мероприятия по идентификации рисков, оценке рисков, мониторингу рисков, в том числе реагированию на риски, подготовке отчетности о рисках.

2.10. Идентификация рисков предусматривает выполнение следующих мероприятий не реже одного раза в год:

- формирование и поддержание в актуальном состоянии перечня бизнес-процессов;
- выявление риск-событий и определение для каждого из выявленных риск-событий величины риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации;
- разработка и поддержка в актуальном состоянии классификаторов рисков в Системе, риск-событий и причин риск-событий.

2.11. Оценка рисков проводится Оператором с учетом рисков, возникающих в связи с привлечением поставщиков услуг, в том числе обусловленных вероятностью невыполнения поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг. Риски, возникающие в связи с привлечением поставщиков 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, идентифицируются в соответствии с пунктом 2.10 настоящего Порядка.

2.12. Оценка рисков в Системе предусматривает следующие мероприятия:

- проведение анализа бизнес-процессов, в том числе анализа программных и (или) технических средств Операторов УПИ, учитывая факт привлечения ими поставщиков услуг, и других факторов, влияющих на БФПС;
- формирования перечня риск-событий для каждого бизнес-процесса с указанием причин риск-событий и их последствий;

- определение для каждого из выявленных рисков в Системе уровня присущего риска до применения способов управления рисками в Системе и установление уровня допустимого риска;
- определение значимых рисков в Системе путем сопоставления уровня присущего риска до применения Способов управления рисками в Системе и уровня допустимого риска по каждому из выявленных рисков в Системе;
- применение Способов управления рисками для каждого из значимых рисков в Системе, и последующее определение для них уровня остаточного риска после применения Способов управления рисками в Системе с целью определения уровня остаточного риска для каждого из значимых для Системы рисков;
- сопоставление уровней остаточного риска после применения Способов управления рисками в Системе и уровня допустимого риска для каждого из значимых рисков в Системе и принятие решения о необходимости применения других Способов управления рисками в Системе в дополнение к ранее примененным способами допустимого уровня рисков для каждого из значимых для Системы рисков для принятия решения о необходимости применения дополнительных Способов управления рисками в Системе.

2.13. Результат идентификации и оценки рисков в Системе отражается в профиле рисков. Перечень информации, содержащейся в профиле рисков, указан в Приложении 5.4 к настоящему Порядку.

2.14. Оператор составляет и пересматривает (актуализирует) профиль каждого из значимых рисков в Системе, включая профиль риска нарушения БФПС, который составляется как сводный профиль в отношении всех значимых рисков в Системе.

2.15. Оператор составляет и пересматривает (актуализирует) профиль рисков, включая профиль риска нарушения БФПС, по результатам плановой или внеплановой оценки всех рисков в Системе, а также внеплановой оценки отдельных рисков (отдельного риска) в Системе.

2.16. Оператор обеспечивает хранение сведений, содержащихся в профиле рисков, не менее пяти лет со дня составления и пересмотра (актуализации) профиля рисков.

2.17. Постоянный анализ рисков достигается путем наблюдения за функционированием Системы, выявления риск-событий, определенных в профиле рисков Системы, либо идентификации новых риск-событий, требующих оценки и пересмотра профиля рисков Системы.

2.18. Мониторинг рисков осуществляется путем наблюдения за соответствием уровня остаточного риска после применения Способов управления рисками уровню допустимого риска при возникновении новых риск-событий и расчета и анализа динамики изменения значений КИР.

2.19. Оценка эффективности мероприятий по восстановлению оказания УПИ в Системе осуществляется посредством сопоставления фактического времени восстановления оказания УПИ, в случае приостановления оказания, и фактического времени восстановления УПИ в соответствии с требованиями к оказанию услуги.

2.20. Решение об эффективности мероприятий по управлению рисками и БФПС принимает исполнительный орган Оператора на основании отчёта, подготовленного ответственным за СУР. Мероприятия по управлению значимыми рисками и непрерывностью функционирования Системы признаются неэффективными при двукратном и более превышении времени восстановления оказания УПИ, установленного Оператором. В иных случаях управление значимыми рисками и непрерывностью функционирования Системы признаются эффективными.

2.21. Оператор вносит изменения в СУР Системы в случае, если действующая система управления рисками в Системе не обеспечила три и более раза в течение календарного года возможность восстановления оказания УПИ в течение периодов времени, установленных Оператором, при их приостановлении.

3. Управление непрерывностью функционирования Системы.

3.1. Управление непрерывностью осуществляется посредством выявления риск- событий, их регистрации в реестре событий риска, оценки влияния на БФПС каждого инцидента, применение мер, в том числе Плана ОНиВД, в отношении инцидентов. Сценарии реагирования в случае реализации инцидента (ИБ, сбой инфраструктуры, инциденты поставщиков и др.) определяются в Плане ОНиВД. При их активации Оператор действует в соответствии с процедурами, описанными в Плане.

3.2. Регистрация инцидентов осуществляется посредством сбора и обработки следующих сведений об инциденте:

- время и дата возникновения инцидента (в случае невозможности установить время возникновения инцидента указывается время его выявления);
- краткое описание инцидента (характеристика произошедшего риск-события 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;
- наличие (отсутствие) факта приостановления (прекращения) оказания УПИ в результате инцидента;
- влияние инцидента на БФПС;
- степень влияния инцидента на функционирование Платежной Системы в зависимости от количества операторов УПИ, и (или) количества и значимости Участников, на которых оказал непосредственное влияние инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников;
- время и дата восстановления оказания УПИ в случае приостановления их оказания;
- мероприятия по устранению неблагоприятных последствий инцидента с указанием планируемой и фактической продолжительности проведения данных мероприятий;
- дата восстановления оказания УПИ, соответствующего требованиям к оказанию услуг;
- неблагоприятные последствия инцидента по Субъектам Платежной Системы, в том числе:
    - сумма денежных средств, уплаченных Оператором и (или) взысканных с Оператора;

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

3.3. Оператор собирает сведения об инцидентах с Субъектов Платежной Системы в соответствии с перечнем, указанным в п. 3.2.

3.4. Оператор рассчитывает фактические значения КИР, анализируемые за предыдущий календарный месяц, не позднее пятого рабочего дня, следующего за окончанием анализируемого календарного месяца.

3.5. По результатам ежемесячной оценки Оператор составляет отчет о сведениях по инцидентам, возникшим при оказании УПИ, и значениям КИР, анализирует динамику изменения значений КИР, рассчитываемых за месяц, и составляет график изменения значений КИР. Указанный отчет является частью набора отчетов оценки СУР в Платежной Системе.

3.6. В случае если вследствие произошедшего в Платежной Системе инцидента нарушен регламент выполнения процедур, но при этом не нарушен пороговый уровень каждого из показателей П1, П2, данный инцидент признается непосредственно не влияющим на БФПС в соответствии с требованиями Положения Банка России № 607-П.

3.7. В случае, если вследствие инцидента в Платежной Системе реализовано хотя бы одно из перечисленных ниже условий, данный инцидент признается непосредственно влияющим на БФПС:

- нарушен регламент выполнения процедур при одновременном нарушении порогового уровня показателя П2;
- нарушен пороговый уровень показателя П1;
- превышена продолжительность установленного Оператором времени, в течение которого должно быть восстановлено оказание УПИ, соответствующее требованиям к оказанию услуг.
- произошло одновременное нарушение пороговых уровней показателей П3, П4, П5 в соответствии с требованиями Положения Банка России № 607-П.

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

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

3.10. В случае выявления дополнительных обстоятельств инцидентов, произошедших в течение месяца, по которому была завершена оценка, Оператор проводит повторную оценку влияния на БФПС с учетом вновь выявленных обстоятельств за данный месяц в течение пяти рабочих дней после завершения месяца, в котором выявлены новые обстоятельства инцидента.

3.11. Если Участник приостановил свою деятельность в Системе по причинам возникновения риск-события у самого Участника, то такое риск-событие не рассматривается Оператором как инцидент.

3.12. Оператор устанавливает порядок оценки качества функционирования операционных и технологических средств, информационных систем:

- каждые два года Оператор проводит оценку качества функционирования операционных и технологических средств и информационных систем Системы путем привлечения независимой организации;
- Оператор самостоятельно осуществляет выбор привлекаемой независимой организации;
- в случае предоставления такой независимой организации конфиденциальной информации для целей проведения оценки качества функционирования операционных и технологических средств и информационных систем Системы Оператор обязан заключить с такой независимой организацией соглашение о неразглашении конфиденциальной информации;
- в результате проведения оценки качества функционирования операционных и технологических средств и информационных систем Системы независимой организацией Оператор вправе принимать решение об изменении операционных и технологических средств и процедур Системы;
- Участники и Операторы УПИ вправе по своему усмотрению и за свой счет проводить оценку качества функционирования операционных и технологических средств и информационных систем на стороне Участников и Операторов УПИ с привлечением независимых организаций.

3.13. Оператор устанавливает порядок изменения операционных и технологических средств и процедур:

- Оператор вправе изменять операционные и технологические средства и процедуры по своему усмотрению в следующих случаях:
    - в случае изменения порядка оказания услуг или вида услуг;
    - в случаях, предусмотренных законодательством Российской Федерации;
    - по требованию Банка России;
    - в рамках СУР;
    - в результате проведения оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;

- В случае если изменение операционных и технологических средств и процедур Оператором требует внесения изменений в Правила, Оператор вносит соответствующие изменения в порядке, предусмотренном Правилами.

- В случае если изменение операционных и технологических средств и процедур Оператором приводит к изменению условий Оферты, Оператор направит Участнику новую Оферту об изменении в порядке, предусмотренном Правилами.

- В случае если изменение операционных и технологических средств и процедур Оператором не требует внесения изменений в Правила и не приводит к изменению условий Оферты, Оператор направляет Участникам уведомление об изменении

операционных и технологических средств и процедур с описанием таких изменений не позднее, чем за тридцать календарных дней до даты вступления в силу соответствующих изменений.

- Участник вправе самостоятельно вносить изменения в операционные и технологические средства и процедуры по взаимодействию с Системой на стороне Участника в случае, если внесение таких изменений не противоречит Правилам Системы, условиям Оферты, законодательству Российской Федерации и не приводит к изменению порядка оказания услуг, предусмотренного Правилами, а также к объему и характеру услуг, оказываемых Участникам.

3.14. Оператор устанавливает порядок привлечения другого Оператора УПИ и перехода Участников на обслуживание к вновь привлеченному Оператору УПИ:

- при наличии в Системе одного Оператора УПИ (Операционного и/или Расчетного центра) Оператор обеспечивает привлечение другого Оператора УПИ и переход Участников на обслуживание к вновь привлеченному Оператору УПИ в случаях:
  - превышения Оператором УПИ времени восстановления оказания УПИ при приостановлении их оказания более двух раз в течение трех месяцев подряд;
  - нарушения Правил, выразившегося в отказе Оператора УПИ в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Системе в случаях, предусмотренных Правилами;

- максимальный срок, в течение которого реализуются мероприятия по привлечению другого Оператора УПИ – шесть месяцев с момента выявления обстоятельств, требующих замену Оператора УПИ.

- переход Участников на обслуживание к привлеченному Оператору УПИ осуществляется в течение шести месяцев с момента регистрации информации о привлеченном Операторе УПИ в Реестре операторов платежных систем.

3.15. Оператор определяет основные требования к обеспечению БФПС Субъектами Системы:

- Субъекты Системы совместно осуществляют деятельность по обеспечению БФПС в Системе, при этом функции контроля находится у Оператора;

- Для обеспечения БФПС Оператор обязан обеспечивать:
  - собственную финансовую устойчивость, поддержание ликвидности;
  - сбор, систематизацию и хранение информации о переводах денежных средств в соответствии с требованиями законодательства и Правилами;
  - принятие мер, направленных на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих оказание УПИ, включая услуги платежного клиринга;
  - принятие профилактических мер (выполнение регламентов) для технологических средств, устройств, информационных систем, обеспечивающих оказание УПИ, включая услуги платежного клиринга и расчетные услуги;
  - принятие мер по отказоустойчивости операционных и технологических средств, устройств и информационных систем при возникновении инцидентов,

повлекших приостановление оказания операционных услуг, и (или) услуг платежного клиринга, и (или) расчетных услуг;
- проведение анализа причин нарушения функционирования операционных и технологических средств, устройств и информационных систем, выработку мер по их устранению;
- соблюдение регламента, определенного для операционных услуг, услуг платежного клиринга и расчетных услуг Системы;
- общий контроль за функционированием Системы и обеспечением БФПС;
- проведение оценки влияния инцидентов на БФПС в соответствии с методикой, установленной в настоящем Порядке;
- проведение мероприятий по восстановлению оказания УПИ в случае возникновения инцидентов, повлекших приостановление оказания операционных услуг, и (или) услуг платежного клиринга, и (или) расчетных услуг, в соответствии с установленным регламентом (Приложение 5.1 к настоящему Порядку);
- проведение оценки СУР в Системе;
- проведение мероприятий по недопущению нарушения БФПС, в том числе связанных с риском потери ликвидности, кредитный риском, правовым риском, операционным риском, общим коммерческим риском;
- проведение прочих мероприятий по своему усмотрению, направленных на обеспечение БФПС;

- для обеспечения БФПС Участники обязаны обеспечивать:
  - собственную финансовую устойчивость, поддержание ликвидности;
  - принятие мер, направленных на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих оказание услуг;
  - принятие профилактических мер (выполнение регламентов) для технологических средств, устройств, информационных систем, обеспечивающих оказание услуг;
  - принятие мер по отказоустойчивости операционных и технологических средств, устройств и информационных систем при возникновении инцидентов в работе Участника;
  - проведение анализа причин нарушения функционирования операционных и технологических средств, устройств и информационных систем, выработку мер по их устранению на стороне Участника;
  - соблюдение регламента, определенного для Участника;
  - своевременное информирование Оператора об инцидентах, касающихся функционирования Системы;
  - проведение мероприятий по восстановлению оказания услуг Участником в случае возникновения инцидентов;
  - проведение прочих мероприятий, направленных на обеспечение БФПС, по своему усмотрению, не противоречащих требованиям законодательства Российской Федерации, нормативным документам Банка России и настоящему Порядку.

3.16. Оператор определяет регламенты для Субъектов Системы в следующих документах:
- в Правилах;
- в Порядке;
- в договорах с Субъектами Системы и/или в офертах;

- в инструкциях, предоставленных Оператором Субъектам Системы.

3.17. Оператор устанавливает порядок перехода на резервный комплекс программных и (или) технических средств:

- Запланированный переход на резервный комплекс программных и (или) технических средств осуществляется в соответствии с заранее установленным графиком при заблаговременном уведомлении об этом пользователей, в том числе Оператора, Участников Системы и привлеченных Операторов УПИ в соответствии с Правилами и (или) иными документами Оператора и (или) привлеченных Операторов УПИ;

- При выходе из строя основного комплекса программных и (или) технических средств осуществляется:
    - Перевод пользователей на резервный комплекс программных и (или) технических средств:
    - с использованием горячего резервного копирования при наличии;
    - при невозможности перехода на резервный комплекс с горячим резервным копированием реализуется схема перевода пользователей на работу с комплексом с использованием холодного резервного копирования;
    - Определение вышедшей из строя компоненты и восстановление основного комплекса программных и (или) технических средств;
    - Перевод пользователей на основной комплекс программных и (или) технических средств.

3.18. Оператор проводит следующие мероприятия, осуществляемые в случае неработоспособности систем и сервисов поставщиков услуг, нарушение предоставления которых способно привести к приостановлению оказания УПИ:

- Формирование рабочей группы из числа сотрудников Оператора и привлеченных экспертов для проведения мероприятий по анализу оценке события, восстановлению процессов, нарушенных вследствие неработоспособности систем и сервисов поставщиков услуг;
- Анализ причин и последствий события, проведение оценки влияния на события на УПИ и БФПС;
- Информирование Участников Системы и Банка России в случае приостановления оказания УПИ в соответствии с пунктом 4.9 главы 4 настоящего Порядка;
- Переключение на услуги резервного поставщика услуг при наличии такого поставщика услуг для затронутого процесса, либо поиск нового поставщика, оказывающего аналогичные услуги, если применимо;
- Проведение восстановительных мероприятий совместно с поставщиком услуг по восстановлению оказания УПИ, если событие, связанное с неработоспособностью систем и сервисов поставщика услуг, оказало влияние на оказание УПИ;
- Разработка рекомендаций для поставщика услуг, допустившего неработоспособность систем и сервисов, нарушение предоставления которых способно привести к приостановлению оказания УПИ;
- Проведение анализа истории событий, связанных с неработоспособностью систем и сервисов поставщика услуг, нарушение предоставления которых привело к приостановлению оказания УПИ;

- Проведение мероприятий по недопущению возникновения подобных событий в будущем.

3.19. Оператор устанавливает порядок обеспечения взаимозаменяемости Операторов УПИ, выполняющих функцию Расчетных центров при наличии в Платежной Системе нескольких Расчетных центров:

- Участник Системы обязан иметь банковский счет не менее чем в двух Расчетных центрах для целей восстановления оказания УПИ в случае возникновении риск-событий, повлекших сбой в оказании услуг;
- в случае принятия Участником Системы решения об осуществлении расчетов через альтернативный Расчетный Центр, Участник уведомит о таком решении Оператора в письменном виде не менее чем за два рабочих дня до планируемой даты начала расчетов через альтернативный Расчетный Центр;
- в случае приостановления оказания УПИ Расчетным Центром, Расчетный Центр, приостановивший оказание УПИ, обязан проинформировать Оператора о приостановлении оказания УПИ в течение 1 часа с момента приостановления оказания УПИ. Начиная с 2 часов после приостановления оказания УПИ альтернативный Расчетный Центр обеспечивает осуществление услуг единственного Расчетного Центра до восстановления оказания УПИ в соответствии с требованиями к оказанию услуг;
- в течение 2 часов после устранения причин приостановления оказания УПИ в соответствии с требованиями оказания услуг Расчетный Центр, который устранил такие причины, обязан уведомить Оператора о восстановлении оказания УПИ в соответствии с требованиями оказания услуг. Начиная со следующего рабочего дня услуги Расчетного центра переходят в штатный режим, действующий до приостановления оказания УПИ в одном из Расчетных центров;
- координацию возврата в штатный режим, а также уведомление Участников о соответствующих изменениях в оказании услуг осуществляет Оператор.

4. Организация взаимодействия Субъектов Системы по обеспечению БФПС.

4.1. В соответствии с Правилами Оператор может запрашивать у Субъектов Системы информацию, касающейся деятельности в качестве Субъекта Системы для целей оценки рисков и влияния на БФПС в Системе в форме адресных запросов и/или интервью и/или анкетирования;

4.2. Субъекты Системы обязаны предоставить Оператору запрашиваемую информацию (в том числе в форме анкетирования), если это не противоречит требованиям законодательства Российской Федерации;

4.3. В случае если запрашиваемая информация содержит сведения, составляющие коммерческую или иную охраняемую законом тайну Субъекта Системы, Оператор обязуется обеспечить сохранение такой информации в соответствии с требованиями законодательства Российской Федерации и Правилами;

4.4. Оператор имеет право предоставлять информацию о БФПС третьим лицам в следующих случаях:

- предусмотренных законодательством Российской Федерации;
- если информация является публичной;

- если получено предварительное письменное согласие владельца информации;
- в случаях, предусмотренных Правилами.

4.5. В случае выявления Оператором нарушений в части обеспечения БФПС Субъектом Системы Оператор информирует Субъекта Системы о таком факте в день выявления Оператором нарушения посредством направления соответствующего сообщения по электронной почте в адрес такого Субъекта Системы;

4.6. Оператор осуществляет проверку устранения нарушений Субъектом Системы в части обеспечения БФПС доступными способами, в том числе, в случае наличия такой возможности, проверку доступности оказываемой Субъектом Системы услуги;

4.7. Субъекты Системы вправе запрашивать разъяснения процедур, отраженных в настоящем Порядке;

4.8. Субъекты Системы вправе вносить предложения в усовершенствование процедур обеспечения БФПС, а Оператор обязан рассматривать вносимые предложения.

4.9. Порядок информирования Банка России и Субъектов Системы о приостановлении и восстановлении оказания УПИ. Оператор информирует:

- Банк России в порядке, предусмотренном законодательством Российской Федерации и документами Банка России;
- Субъекты Системы о случаях и причинах приостановления (прекращения) оказания УПИ в день такого приостановления (прекращения) путем направления соответствующего уведомления по электронной почте на адрес Субъекта Системы;
- По факту восстановления обеспечения УПИ в Системе Оператор уведомляет об этом Субъектов Системы и Банк России в день восстановления путем направления соответствующего уведомления по электронной почте на адрес Субъекта Системы.

4.10. Отчетность по БФПС в Банк России.

4.10.1. Общие требования к отчетности

Оператор обеспечивает подготовку и представление в Банк России отчетности по БФПС в соответствии с требованиями Указания Банка России № 5110-У «О форме и сроках предоставления в Банк России отчетности оператора услуг платежной инфраструктуры, оператора платежной системы по инцидентам, возникшим (выявленным) при оказании услуг платежной инфраструктуры, показателям бесперебойности функционирования платежной системы и методике ее составления».

4.10.2. Состав отчетности.

Отчетность по БФПС включает:
- отчет по инцидентам, возникшим при оказании УПИ;
- отчет по показателям БФПС (П1-П5);
- информацию о значениях ключевых индикаторов риска;
- сведения об оценке влияния инцидентов на БФПС.

4.10.3. Периодичность и сроки представления.

- Ежемесячная отчетность - до 10 числа месяца, следующего за отчетным;
- Внеплановая отчетность - при возникновении существенных инцидентов, влияющих на БФПС, в течение 1 рабочего дня;
- Годовая отчетность - до 31 января года, следующего за отчетным.

4.10.4. Ответственность за отчетность

Ответственным за подготовку, контроль качества и своевременное представление отчетности по БФПС в Банк России назначается исполнительный орган Оператора или уполномоченное им лицо.

4.11. Порядок взаимодействия в спорных, нестандартных и чрезвычайных ситуациях.

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

- Субъекты Системы освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств, если это неисполнение или ненадлежащее исполнение явилось следствием обстоятельств непреодолимой силы, возникших после вступления в силу Правил, в результате событий чрезвычайного характера, которые Субъекты Системы не могли ни предвидеть, ни предотвратить разумными мерами;

- К обстоятельствам непреодолимой силы относятся риск-события, на которые Субъекты Системы 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 Системы своих обязательств;

- Субъект Системы, для которого в связи с наступлением обстоятельств непреодолимой силы создалась невозможность исполнения своих обязательств, должен не позднее следующего рабочего дня уведомить других Субъектов Системы о дате наступления и о предполагаемой дате прекращения указанных обстоятельств непреодолимой силы; Субъект Системы, находящийся под воздействием обстоятельств непреодолимой силы, имеет право приостановить исполнение своих обязательств до прекращения действия обстоятельств непреодолимой силы;

- Уведомление о наступлении обстоятельств непреодолимой силы направляется Субъектами Системы следующим образом:

- Участник, находящийся под воздействием обстоятельств непреодолимой силы, направляет уведомление Оператору;
- Оператор, находящийся под воздействием обстоятельств непреодолимой силы, направляет уведомление всем Субъектам.

4.12. В случае возникновения споров между Субъектами Системы такие споры разрешаются в порядке, предусмотренном Правилами.

5. Контроль за соблюдением Субъектами Системы БФПС.

5.1. Оператор осуществляет контроль порядка обеспечения БФПС Субъектами Системы следующими способами:

- сбор, документирование и анализ сведений об инцидентах, получаемых от Субъектов Системы;
- использование сведений об инцидентах в оценках СУР и обеспечения БФПС;
- оценка динамики изменения количества инцидентов посредством расчета соответствующих КИР;
- детальный анализ существенных инцидентов, причин их возникновения, сроков устранения;
- анкетирование и/или интервью и/или адресные запросы, проведение самооценки Субъектов Системы с целью получения сведений, необходимых для использования в мероприятиях по контролю порядка обеспечения БФПС Субъектами Системы;
- направление запросов ОУПИ на предоставление внутренних документов по БФПС;
- работа с информацией по жалобам клиентов;
- оценка СУР;
- контроль финансового состояния Субъектов Системы;
- тестирование доступности оказания УПИ, в том числе доступности УПИ Участников.

5.2. Оператор доводит до сведения Субъектов Системы информацию о выявленных недостатках в области обеспечения БФПС и рекомендации по их устранению по доступным каналам связи по выбору Оператора.

6. Организационная структура обеспечения БФПС.

6.1. Организационная структура для обеспечения бесперебойности функционирования Платежной Системы включает следующие уровни:

- Исключительный уровень управления рисками в Системе, а также обеспечения бесперебойности функционирования Платежной Системы – собрание участников Оператора;

- На первом уровне управления рисками в Системе, а также обеспечения бесперебойности функционирования Системы действуют:
  - сотрудники структурных подразделений, осуществляющие бизнес-процессы Системы, ответственные за управление рисками и обеспечение бесперебойности функционирования в Системе в рамках своих полномочий, определенных должностными инструкциями, внутренними документами и приказами (далее «СПоБП»);

- На втором уровне управления рисками в Платежной Системе, а также обеспечения бесперебойности функционирования Платежной Системы действуют:
    - исполнительный орган Оператора;
    - руководители структурных подразделений, осуществляющих бизнес-процессы Системы, ответственных за управление рисками и обеспечение бесперебойности функционирования в Системе в рамках своих полномочий, определенных должностными инструкциями, внутренними документами и приказами (далее «Руководители СПоБП»);

6.2. Обеспечение БФПС первого уровня организационной структуры Системы выполняется СПоБП при выполнении ими бизнес-процессов Системы, в том числе при выполнении и (или) координации ими работ в рамках своих полномочий.

6.3. Обеспечение БФПС второго уровня организационной структуры Системы выполняется руководителями СПоБП и исполнительным органом Оператора в части контрольных и организационных мероприятий, а также при принятии решений о БФПС в рамках своих полномочий.

6.4. Руководители СПоБП выполняют следующие функции:
- осуществляют контроль за обеспечением БФПС своими структурными подразделениями;
- принимают решение о реагировании на инциденты в зависимости от степени воздействия на УПИ, в том числе опринятии ответных мер и активации сценариев Плана ОНиВД (за исключением решений, которые относятся к компетенции Правления);
- обеспечивают формирование и поддержание в актуальном состоянии описания бизнес-процессов;
- совместно с Ответственным за БФПС обеспечивают идентификацию рисков, присущих бизнес-процессам;
- совместно с Ответственным за БФПС обеспечивают проведение оценки значимых рисков;
- обеспечивают осведомленность своих сотрудников СПоБП о значимых рисках и порядке управления ими в соответствии с разработанными внутренними документами;
- разрабатывают внутренние инструкции, методики, положения для СПоБП на основе методик и процедур, определенных сотрудниками второго уровня;
- предоставляют информацию для составления профиля рисков и согласовывают сведения в профиле рисков, составленный на основании проведенной оценки;
- предоставляют предложения о реагировании на значимые риски;
- обеспечивают подготовку, тестирование и пересмотр Плана ОНиВД в рамках своей зоны ответственности за бизнес-процессы и системы;
- направляют предложения по дополнительным КИР (если требуется их введение) и обеспечивают выполнение установленных КИР;
- обеспечивают предоставление информации для анализа рисков Платежной Системы;
- обеспечивают выявление и регистрацию риск-событий;
- обеспечивают полноту и корректность сведений о зарегистрированных риск- событиях;
- обеспечивают своевременное доведение информации о риск-событиях и БФПС до сотрудников организационной структуры Платежной Системы второго уровня;
- предоставляют информацию по риск-событиям для оценки влияния на БФПС;

- предоставляют информацию для отчетов о БФПС.

6.5. Исполнительный орган Оператора выполняет следующие функции:

- утверждает Порядок обеспечения БФПС;
- утверждает профиль рисков Платежной Системы;
- рассматривает отчеты о БФПС;
- принимает решения о реагировании на инциденты в зависимости от степени воздействия на УПИ;
- согласовывает предложения по Способам управления рисками;
- согласовывает предложения по дополнительным КИР (если требуется их введение);
- обеспечивает принятие решений о применении Способов управления рисками с целью обеспечение непрерывности функционирования Платежной Системы в условиях риск-события при приостановлении оказания УПИ на срок, превышающий допустимый уровень, в том числе об активации сценариев Плана ОНиВД;
- принимает решение по спорным вопросам, по вопросам с отсутствующей согласованной позицией сотрудников первого уровня организационной структуры Платежной Системы;
- организуют процедуру информирования заинтересованных лиц о влиянии на БФПС с учетом установленных порядков;
- утверждает отдельные процедуры по управлению рисками в Платежной Системе в рамках своих полномочий и в соответствии с настоящим Порядком;
- распределяет полномочия, обязанности и ответственность между структурными подразделениями в области управления рисками и обеспечения БФПС.

Приложение 5.1. Регламент выполнения процедур в Системе.

| **Наименование УПИ** | **Наименование процедуры** | **Время выполнения процедуры УПИ** |
|---|---|---|
| Операционная услуга | Приём и обработка распоряжения по отправке или выплате переводов денежных средств в Систему (включая контрольные процедуры по приему/выдаче распоряжения). | Не более 5 минут |
| Услуга платежного клиринга | Расчет платежных клиринговых позиций Участников. Формирование реестров ПКЦ. | С 00:00 Мск до 08:00 Мск суток, следующих за сутками приема распоряжения по отправке или выплате переводов денежных средств в Системе. |
| | Предоставление реестров ПКЦ Участникам по всем распоряжениям Участников, принятым в Систему. | С 08:00 Мск до 08:30 Мск суток, следующих за сутками приема распоряжения по отправке или выплате переводов денежных средств в Системе. Время окончания процедуры: не позднее 08:30 Мск этих же суток. |
| | Подготовка и передача в Расчетный центр реестров ПКЦ. | С 08:00 Мск до 08:30 Мск суток, следующих за сутками приема распоряжения по отправке или выплате переводов денежных средств в Системе. |
| Расчетная услуга | Проведение расчетов. Исполнение платежных клиринговых позиций согласно полученному реестру при условии достаточности остатка денежных средств на корреспондентских счетах Участников для проведения соответствующих платежных клиринговых позиций. | С 08:30 Мск до 11:00 Мск суток, следующих за сутками приема распоряжения по отправке или выплате переводов денежных средств в Системе. |

Приложение 5.2. Уровни ключевых индикаторов риска.

Для оценки риска БФПС в соответствии с требованиями используются следующие ключевые индикаторы риска:

П1 - показатель продолжительности восстановления оказания УПИ, 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 нормативными документами Банка России;

П2 - показатель непрерывности оказания УПИ, характеризующий период времени между двумя последовательно произошедшими в Платежной Системе риск-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, в результате которых приостанавливалось оказание УПИ.

П3 - показатель соблюдения регламента (далее «показатель П3»), характеризующий соблюдение Операторами УПИ времени начала, времени окончания, продолжительности и последовательности процедур, выполняемых Операторами УПИ при оказании операционных услуг, услуг платежного клиринга и расчетных услуг;

П4 - показатель доступности Операционного Центра Системы (далее «показатель П4»), характеризующий оказание операционных услуг Операционным Платежной Системы;

П5 - показатель изменения частоты инцидентов (далее «показатель П5»), характеризующий темп прироста частоты инцидентов.
Порядок расчета показателей и их пороговые значения

1. 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. Пороговый уровень показателя П1 <= 6 часов.

2. 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 более одного вида УПИ одновременно, то показатель П2 рассчитывается одновременно по всем видам УПИ, оказываемым данным Оператором УПИ.

Показатель П2 рассчитываться в часах/минутах/секундах. Пороговый уровень показателя П2 >= 6 часов;

3. Показатель П3 рассчитывается по каждому Оператору УПИ.

Для Операционного Центра показатель П3 рассчитывается как отношение количества распоряжений Участников (их клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников (их клиентов), по которым были оказаны операционные услуги в течение календарного месяца, рассчитываемое по следующей формуле:

$П3о_{Ц}$ = (Nоц /NT) * 100,

где
Nоц - количество распоряжений Участников (их клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур;
NT - общее количество распоряжений Участников (их клиентов), по которым были оказаны операционные услуги в течение календарного месяца;

Пороговый уровень показателя П3оц >= 98.00%.
Для Платежного Клирингового Центра показатель П3 должен рассчитываться как
отношение количества распоряжений Участников (их клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников (их клиентов), по которым были оказаны УПИ в течение календарного месяца, рассчитываемое по следующей формуле:

$П3пк_{Ц}$ = (Nпкц /NT) * 100,

где
Nпкц - количество распоряжений Участников (их клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур;
NT - общее количество распоряжений Участников (их клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца.

Пороговый уровень показателя П3пкц >= 98.00%.

Для Расчетного Центра показатель П3 должен рассчитываться как отношение количества распоряжений Участников 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 и (или) Платежного Клирингового Центра, по которым были оказаны расчетные услуги в течение календарного месяца, рассчитываемое по следующей формуле:

П3рц = (Nрц /NT) * 100,

где
Nрц - количество распоряжений Участников и (или) Платежного Клирингового Центра, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур;
NT - общее количество распоряжений Участников и (или) Платежного Клирингового Центра, по которым были оказаны расчетные услуги в течение календарного месяца.

Значение показателя П3 по Системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем Операторам УПИ в отношении всех видов оказываемых ими услуг. Если Оператор УПИ оказывает более одного вида УПИ одновременно, показатель П3 рассчитывается по данному Оператору УПИ в отношении всех видов оказываемых им услуг.

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

Пороговый уровень показателя П3рц >= 99.00%.

4. Показатель П4 рассчитывается как среднее значение коэффициента доступности Операционного Центра Платежной Системы за календарный месяц, рассчитываемое по следующей формуле:

$$П\,4 = \left( \sum_{i=1}^{M} \left( 1 - \frac{D_i}{T_i} \right) \Big/ M \right) \times 100\,\%$$

где
M - количество рабочих дней Системы в месяце;
Di - общая продолжительность всех приостановлений оказания операционных услуг Операционным Центром Системы за i-ый рабочий день месяца в минутах;
Ti - 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).

Если в Системе функционирует более одного Операционного Центра показатель П4 рассчитываться для каждого Операционного Центра Системы, а значение показателя П4 по Системе в целом принимается равным наименьшему из значений, рассчитанных по всем Операционным Центрам Системы.

Пороговый уровень показателя П4 >= 96.00%.

5. Показатель П5 рассчитывается по 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

двенадцать календарных месяцев, включая оцениваемый календарный месяц, рассчитываемый по следующей формуле:

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

где

КИi - количество инцидентов в течение i-го рабочего дня Системы оцениваемого календарного месяца;
M - количество рабочих дней Системы в оцениваемом календарном месяце;
N - количество рабочих дней Системы за двенадцать предыдущих календарных месяцев, включая оцениваемый месяц.

Показатель П5 рассчитывается ежемесячно в процентах с точностью до одного знака после запятой (с округлением по математическому методу).

Если за предыдущие двенадцать календарных месяцев, включая оцениваемый месяц, инцидентов не было, значение показателя признается равным нулю. Если за предыдущие двенадцать календарных месяцев, включая оцениваемый месяц, в шести месяцах не было инцидентов, при этом за оцениваемый месяц количество инцидентов не превышает 10, значение показателя признается равным нулю.

Если Оператор УПИ оказывает более одного вида УПИ одновременно, показатель П5 рассчитывается по данному Оператору УПИ в отношении всех видов оказываемых им услуг.

Пороговый уровень показателя П5 <= 300%.

6. Обоснование пороговых уровней показателей БФПС.

Методология установления пороговых уровней:

Пороговые уровни показателей П1-П5 установлены на основе

- требований Положения Банка России № 607-П;
- планируемых операционных возможностей Системы (в связи с тем, что Система находится на стадии внедрения и исторические данные о функционировании отсутствуют);
- анализа технических характеристик используемого оборудования и программного обеспечения;
- лучших практик управления рисками в платежных системах;
- консервативного подхода к управлению рисками с учетом отсутствия операционной статистики.

Пересмотр пороговых уровней:

Установленные пороговые уровни подлежат обязательному пересмотру не реже одного раза в год на основе:

- накопленной статистики функционирования Системы;
- результатов оценки эффективности СУР;
- изменений в операционной среде Системы;
- требований регулирующих органов.

Первый пересмотр пороговых уровней планируется провести через 12 месяцев после начала промышленной эксплуатации Системы.

Ответственным за ежегодный пересмотр пороговых уровней КИР и показателей П1–П5 на основании накопленной статистики, результатов оценки СУР и изменений в операционной среде является исполнительный орган Оператора или уполномоченное им лицо. Решения оформляются приказом Оператора.

Приложение 5.3. Критерии значимости риск событий.

1. Для определения уровня значимого риска в Платежной Системе осуществляется оценка риск-события по матрице чувствительности к риску (вероятности (частоты) реализации риска) и матрице влияния на деятельность Платежной Системы (воздействия риска).

2. Матрица, отражающая уровень чувствительности к риску (вероятности (частоты) реализации риска)

| **Вероятность (частота) возникновения риск-события в бизнес-процессе** | **Качественная оценка** |
|---|---|
| >52 раз в год | Почти точно (4) |
| От 12 до 52 раз в год | Очень вероятно (3) |
| От 3 до 11 раз в год | Возможно (2) |
| <=2 раза в год | Маловероятно (1) |

При определении уровня чувствительности к риску при получении значения, отличного от пороговых величин, выбирается наиболее близкая пороговая величина.

3. Матрица, характеризующая уровень влияния риска на деятельность Системы.

3.1. Критерии существенности по операционным услугам.

Для целей оценки риск-события по критериям существенности для расчета количества операций переводов денежных средств, ожидаемых за календарный день, в котором произошло риск-событие, определяется среднее количество операций переводов денежных средств за предыдущие календарные дни, в которых не было риск-событий, соответствующие по объему оцениваемому календарному дню.

| **Критерий** | **Риск-событие или инцидент** | **Нарушение УПИ** | **Уровни оказания УПИ** |
|---|---|---|---|
| Сбой, не влияющий на приостановление (прекращение) Операционных услуг | Риск-событие (0) | Нет | Штатный режим |
| Сбой, влияющий на 0.01% - 15% количества операций денежных переводов | Риск-событие (0) | Нет | Штатный режим |
| Сбой, влияющий на 15.01% - 20% количества операций денежных переводов | Инцидент низкий (1) | Нет | Штатный режим |
| Сбой, влияющий на 20.01% - 40% количества операций денежных переводов | Инцидент умеренный (2) | Нет | Штатный режим |
| Сбой, влияющий на 40.01% - 90% количества операций денежных переводов | Инцидент средний (3) | Нет | Ограниченный режим |
| Сбой, влияющий на >90.00% количества операций денежных переводов | Инцидент высокий (4) | Да | Приостановление |

Восстановление оказания УПИ в соответствии с требованиями к оказанию услуг достигается при переходе в штатный режим.

3.2. Критерии существенности по услугам Платежного клирингового центра и/или Расчетного центра.

| **Критерий** | **Риск-событие или инцидент** | **Нарушение УПИ** | **Уровни оказания УПИ** |
|---|---|---|---|
| Сбой, не влияющий на оказание услуг Расчетного центра и/или Платежного клирингового центра | Риск-событие (0) | Нет | Штатный режим |
| Сбой, приведший к нарушению требований к оказанию услуг Расчетного и/или Платежного клирингового центра на период до 2 часов в течение операционного дня Оператора УПИ, в котором произошел сбой | Инцидент низкий (1) | Нет | Штатный режим |
| Сбой, приведший к нарушению требований к оказанию услуг Расчетного и/или Платежного клирингового центра на период от 2 до 6 часов в течение операционного дня Оператора УПИ, в котором произошел сбой | Инцидент умеренный (2) | Нет | Штатный режим |
| Сбой, приведший к нарушению требований к оказанию услуг Расчетного и/или Платежного клирингового центра на период от 6 часов до окончания операционного дня Оператора УПИ, в котором произошел сбой | Инцидент средний (3) | Нет | Ограниченный режим |
| Сбой, приведший к приостановлению услуг Расчетного и/или Платежного клирингового центра свыше операционного дня Оператора УПИ, в котором произошел сбой | Инцидент высокий (4) | Да | Приостановление |

Восстановление оказания УПИ в соответствии с требованиями к оказанию услуг достигается при переходе в штатный режим.

3.3. Критерии существенности по риск-событиям информационной безопасности.

| Критерий | Риск-событие или инцидент | Нарушение УПИ | Уровни оказания УПИ |
|---|---|---|---|
| Риск-событие, нарушившее информационную безопасность в инфраструктуре Участника (отсутствуют потери третьих лиц и/или Оператора, отсутствует влияние на УПИ. | Риск-событие (0) | Нет | Штатный режим |
| Риск-событие, нарушившее информационную безопасность в инфраструктуре Участника (присутствуют потери третьих лиц, отсутствует влияние на операционные и/или платежные клиринговые и/или расчетные услуги) | Риск-событие (0) | Нет | Штатный режим |
| Риск-событие, нарушившее информационную безопасность в инфраструктуре Участника (имеются потери третьих лиц, обращенные к Оператору, отсутствует влияние на операционные и/или платежные клиринговые и/или расчетные услуги) | Инцидент низкий (1) | Нет | Штатный режим |
| Риск-событие, нарушившее информационную безопасность в инфраструктуре Оператора и/или Оператора УПИ (отсутствуют потери третьих лиц и/или Оператора, отсутствует влияние на операционные и/или платежные клиринговые и/или расчетные услуги) | Инцидент умеренный (2) | Нет | Штатный режим |
| Риск-событие, нарушившее информационную безопасность в инфраструктуре Оператора и/или Оператора УПИ (имеются потери третьих лиц и/или Оператора, отсутствует влияние на операционные и/или платежные клиринговые и/или расчетные услуги) | Инцидент средний (3) | Нет | Ограниченный режим |
| Риск-событие, нарушившее информационную безопасность в инфраструктуре Оператора и/или Оператора УПИ (имеются потери третьих лиц и/или Оператора, имеется влияние на операционные и/или платежные клиринговые и/или расчетные услуги) | Инцидент высокий (4) | Да | Приостановление |

Восстановление оказания УПИ в соответствии с требованиями к оказанию услуг достигается при переходе в штатный режим.

3.4. По рискам, находящимся в зеленой или желтой зонах, решение о применении мер реагирования принимается на первом уровне управления; по рискам, находящимся в оранжевой

и красной зонах, решение о применении мер реагирования принимается на втором уровне управления. Прочие риск-события рассматриваются как не влияющие на УПИ.

4. Показатели уровня риска информационной безопасности участника Платежной системы СБК

4.1. Настоящий раздел определяет состав и пороговые значения показателей уровня риска информационной безопасности (далее – показатели уровня риска ИБ) участника Платежной системы СБК (далее – Участник ПС), а также порядок их расчёта и контроля в соответствии с требованиями подпункта 2.3.5 пункта 2.3 Положения Банка России от 03.10.2017 № 607-П и пунктов 5.1, 5.2 Положения Банка России от 17.08.2023 № 821-П.

4.2. Оператор Платежной системы СБК устанавливает следующие показатели уровня риска ИБ Участника ПС:

4.2.1. Показатель КПУР ИБ ОБС (доля) – отношение общего объёма операций по переводу денежных средств, совершённых без добровольного согласия клиентов Участника ПС (далее – операции без согласия), к общему объёму операций по переводу денежных средств Участника ПС за отчётный период (квартал), выраженное в процентах:
КПУР ИБ ОБС (доля) = (Vнесогл / Vобщ) × 100%
где: Vнесогл – объём операций по переводу денежных средств без добровольного согласия клиентов (в рублёвом эквиваленте) за отчётный период; Vобщ – общий объём операций по переводу денежных средств Участника ПС (в рублёвом эквиваленте) за отчётный период.
Под операциями без добровольного согласия клиента понимаются операции, совершённые без согласия клиента или с согласия клиента, полученного под влиянием обмана или при злоупотреблении доверием.

4.2.2. Показатель КПУР ИБ ОБС (количество) – отношение количества операций по переводу денежных средств, совершённых без добровольного согласия клиентов Участника ПС, к общему количеству операций по переводу денежных средств Участника ПС за отчётный период (квартал), выраженное в процентах:
КПУР ИБ ОБС (количество) = (Nнесогл / Nобщ) × 100%
где: Nнесогл – количество операций по переводу денежных средств без добровольного согласия клиентов за отчётный период; Nобщ – общее количество операций по переводу денежных средств Участника ПС за отчётный период.

4.2.3. Показатель КИР ИБ (инциденты) – количество инцидентов защиты информации, выявленных Участником ПС и повлиявших на оказание услуг платежной инфраструктуры в Платежной системе СБК, за отчётный период (квартал).

4.3. Пороговые значения показателей уровня риска ИБ Участника ПС устанавливаются Оператором Платежной системы СБК в следующем размере:

| № | Показатель | Что измеряет | Формула | Пороговое значение |
|---|---|---|---|---|
| 1 | КПУР ИБ ОБС (доля) | Доля объёма операций без согласия клиента в общем | (Vнесогл / Vобщ) × 100% | ≤ 0,005% за квартал |
| 2 | КПУР ИБ ОБС (количество) | Доля количества операций без | (Nнесогл / Nобщ) × 100% | ≤ 0,005% за квартал |

| | | | | |
|---|---|---|---|---|
| | | согласия клиента в общем | | |
| 3 | КИР ИБ (инциденты) | Количество инцидентов защиты информации, повлиявших на оказание УПИ | Абсолютное число | ≤ 2 инцидентов за квартал |

Пороговые значения показателей уровня риска ИБ могут пересматриваться Оператором Платежной системы СБК с учётом результатов оценки рисков в платежной системе и рекомендаций коллегиального органа по управлению рисками.

4.4. Порядок расчёта и контроля показателей уровня риска ИБ:

4.4.1. Фактические значения показателей уровня риска ИБ рассчитываются Оператором Платежной системы СБК ежеквартально на основании сведений, представляемых Участниками ПС и операторами услуг платежной инфраструктуры (далее – операторы УПИ), а также сведений, полученных от Банка России, в том числе содержащихся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента.

4.4.2. Участники ПС обязаны представлять Оператору Платежной системы СБК следующие сведения в срок не позднее 15-го рабочего дня месяца, следующего за отчётным кварталом: количество и объём операций по переводу денежных средств за отчётный период; количество и объём операций по переводу денежных средств, совершённых без добровольного согласия клиентов, за отчётный период, с разбивкой по каналам проведения операций; сведения об инцидентах защиты информации, повлиявших или способных повлиять на оказание услуг платежной инфраструктуры.

4.4.3. Оператор Платежной системы СБК осуществляет мониторинг фактических значений показателей уровня риска ИБ путём сравнения их с пороговыми значениями, установленными в пункте 4.3 настоящего раздела.

4.5. Меры реагирования при превышении пороговых значений показателей уровня риска ИБ:

4.5.1. В случае выявления превышения фактическим значением показателя уровня риска ИБ Участника ПС установленного порогового значения Оператор Платежной системы СБК направляет Участнику ПС уведомление о выявленном факте превышения не позднее 5 рабочих дней с даты завершения расчёта показателей.

4.5.2. Участник ПС, в отношении которого выявлено превышение порогового значения показателя уровня риска ИБ, обязан в срок не позднее 20 рабочих дней с даты получения уведомления представить Оператору Платежной системы СБК план мероприятий по снижению уровня риска ИБ с указанием сроков их реализации.

4.5.3. В случае повторного (в течение двух последовательных отчётных периодов) превышения порогового значения показателя уровня риска ИБ Оператор Платежной системы СБК вправе применить в отношении Участника ПС и (или) операторов УПИ ограничения по параметрам операций по осуществлению переводов денежных средств в соответствии с пунктом 5.2 Положения Банка России от 17.08.2023 № 821-П, в том числе: установление ограничений по максимальной сумме перевода денежных средств за одну операцию; установление ограничений

по суммарному объёму переводов денежных средств за определённый период времени; иные ограничения, определённые Правилами Платежной системы СБК.

4.5.4. Ограничения, указанные в пункте 4.5.3, снимаются по решению Оператора Платежной системы СБК после представления Участником ПС подтверждения устранения причин превышения порогового значения показателя уровня риска ИБ и при условии, что фактическое значение соответствующего показателя в следующем отчётном периоде не превышает порогового значения.

4.6. Влияние показателей уровня риска ИБ на оценку инцидентов и БФПС:

4.6.1. Показатели уровня риска ИБ Участников ПС учитываются при определении влияния инцидентов на бесперебойность функционирования Платежной системы СБК в соответствии с подпунктом 2.3.5 пункта 2.3 Положения Банка России от 03.10.2017 № 607-П.

4.6.2. Результаты мониторинга показателей уровня риска ИБ используются при проведении плановой и внеплановой оценки рисков в Платежной системе СБК в соответствии с разделами 2 и 3 настоящего Приложения.

Приложение 5.4. Профиль риска и требования к его заполнению.

Профиль риска формируется в соответствии с требованиями, установленными пунктом 2.7 Положения Банка России № 607-П.

Актуализация профилей рисков

В соответствии с требованиями Положения Банка России № 607-П профили рисков подлежат обязательной актуализации:

- не реже одного раза в год - плановая актуализация;
- при выявлении новых значимых рисков - внеплановая актуализация;
- при изменении бизнес-процессов Системы - внеплановая актуализация;
- по результатам анализа произошедших инцидентов - внеплановая актуализация;
- при изменении нормативных требований Банка России - внеплановая актуализация.

Ответственность за актуализацию профилей рисков возлагается на руководителей структурных подразделений, ответственных за соответствующие бизнес-процессы, под общим контролем исполнительного органа Оператора.

Профили рисков должны составляться по всем значимым рискам в Системе, в том числе по:

1. Правовому риску Системы – риску оказания УПИ, не соответствующих требованиям к оказанию услуг, вследствие

- несоблюдения Субъектами Системы требований законодательства Российской Федерации, Правил, договоров, заключенных между субъектами Платежной Системы, документов Оператора и документов Операторов УПИ;
- наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России, Правилах и договорах, заключенных между субъектами Платежной Системы;
- нахождения Операторов УПИ и Участников под юрисдикцией различных государств).

2. Операционному риску Системы - риску оказания УПИ, не соответствующих требованиям к оказанию услуг, вследствие:

- возникновения у субъектов Системы сбоев, отказов и аварий в работе информационных и технологических систем,
- недостатков в организации и выполнении технологических и управленческих процессов,
- ошибок или противоправных действий персонала субъектов Платежной Системы,
- воздействия событий, причины возникновения которых не связаны с деятельностью субъектов Системы, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц).

3. Кредитному риску Системы - риску оказания УПИ, не соответствующих требованиям к оказанию услуг, Центральным Платежным Клиринговым Контрагентом или Расчетным Центром Платежной Системы вследствие

- невыполнения Участниками договорных обязательств перед указанными организациями в установленный срок или в будущем).

4. Риску ликвидности Платежной Системы - риску оказания УПИ, не соответствующих требованиям к оказанию услуг, вследствие

- отсутствия у Субъектов Системы денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами Системы).

5. Общему коммерческому риску Системы - риску оказания УПИ, не соответствующих требованиям к оказанию услуг, вследствие

- ухудшения финансового состояния Оператора и (или) Операторов УПИ, не связанного с реализацией кредитного риска Системы и риска ликвидности Системы).

Перечень возможных причин возникновения риск-события в Системе

| **Причина возникшего (выявленного) инцидента** | **Код** |
|---|---|
| Нарушения Оператором УПИ бизнес-процессов в Системе, в том числе вследствие ненадлежащей организации бизнес-процессов, нарушения выполнения бизнес-процессов, внутренних регламентов и процедур | 01 |
| Нарушения в работе персонала и в организации труда Оператора УПИ, в том числе вследствие превышения сотрудниками своих полномочий, ошибочных противоправных действий и (или) бездействия персонала | 02 |
| Нарушения в работе систем, оборудования и технологий Оператора УПИ, не связанных с нарушением безопасности и защиты информации, в том числе по причине невыполнения поставщиками (провайдерами) услуг, предоставляющими или поддерживающими системы и сервисы, необходимые для оказания Оператором УПИ услуг платежной инфраструктуры, своих обязательств, включая неработоспособность систем и сервисов поставщиков (провайдеров) услуг | 03 |
| Нарушения в работе систем, оборудования и технологий у Оператора УПИ, связанных с нарушением безопасности и защиты информации, в том числе в результате реализации компьютерных атак | 04 |
| Несоблюдение Правил, договоров об оказании операционных услуг и (или) платежных клиринговых услуг, и (или) договоров банковского счета | 05 |
| Нарушения в деятельности Оператора УПИ по причине обстоятельств непреодолимой силы, в частности стихийных бедствий, технологических катастроф, недобросовестных действий третьих лиц, применения мер организациями и ведомствами, в том числе центральными (национальными) банками иностранных государств в рамках международных санкций | 06 |
| Несоблюдение Правил и (или) договоров, заключенных с Оператором УПИ, об оказании операционных услуг и (или) платежных клиринговых услуг, если заключение таких договоров предусмотрено Правилами | 07 |
| Несоблюдение Участником (Участниками) Правил и (или) договоров об оказании операционных услуг, и (или) платежных клиринговых услуг, и (или) договоров банковского счета, неработоспособность систем и сервисов Участника (Участников) | 08 |
| Несоблюдение операционным центром Платежной Системы Правил и (или) договоров об оказании операционных услуг, если заключение таких договоров предусмотрено Правилами, неработоспособность систем и сервисов | 09 |

| | |
|---|---|
| Несоблюдение Платежным клиринговым центром Платежной Системы Правил и (или) договоров об оказании платежных клиринговых услуг, если заключение таких договоров предусмотрено Правилами, неработоспособность систем и сервисов Платежного клирингового центра Платежной Системы | 10 |
| Несоблюдение Расчетным центром Центральным платежным клиринговым контрагентом Платежной Системы Правил и (или) договоров, заключенных с Операционным центром и (или) Платежным клиринговым центром Платежной Системы, если заключение таких договоров предусмотрено Правилами, договоров банковского счета, заключаемых с Участниками, неработоспособность систем и сервисов Расчетного центра и (или) Центрального платежного клирингового контрагента Платежной Системы | 11 |
| Иные причины возникшего (выявленного) инцидента, не предусмотренные кодами 01 - 11 | 20 |

Основные Способы управления рисками в Платежной Системе по видам рисков.

| **Виды рисков Платежной Системы** | **Способы управления рисками** |
|---|---|
| Правовой риск | Ежедневный мониторинг банковских операций на предмет выявления возможных рисков и несоответствий действующему законодательству;<br>Анализ нормативно-правовой документации на предмет соответствия требованиях законодательства действующих процессов и новых, разрабатываемых процессов и процедур;<br>Периодический инструктаж сотрудников, периодическая проверка знаний сотрудников, доведение до сведений сотрудников изменений в законодательстве и внутренних процедур. |
| Операционный риск | • Разработка технических требований на создание, внедрение и эксплуатацию аппаратно-программных комплексов с учётом требований к показателям бесперебойности;<br>• Тестирование аппаратно-программных комплексов перед их внедрением;<br>• Регулярный мониторинг системного, прикладного программного обеспечения и доступа к информационным ресурсам;<br>• Обеспечение целостности информационных активов путём применения средств идентификации и аутентификации, процедур протоколирования и аудита, криптографической защиты информации, резервного копирования и архивирования информационных ресурсов;<br>• Обеспечение резервирования критичных информационных активов; разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев;<br>• Проведение регулярной оценки качества и надёжности функционирования информационных систем, операционных и технологических средств, соответствие их отраслевым нормативным актам;<br>• Сбор, систематизация, обработка, анализ и хранение информации об инцидентах в Платежной Системе;<br>• Анализ потенциальных источников операционного риска при заключении новых договоров, сделок, разработки новых банковских продуктов, технологий, построение схем, моделей, созданий процедур;<br>• Включение в договоры с Расчетным центром условий об обеспечении бесперебойности функционирования процедур, а также штрафных санкций случае возникновения операционного риска;<br>• Проведение регламентных работ по обеспечению БФПС;<br>• Ограничение функций и полномочий на системном уровне;<br>• Обучение персонала;<br>• Введение скриптов, регламентов и инструкций для персонала. |

| | |
|---|---|
| Кредитный риск | • Автоматизированный контроль остатка на счетах Участников в Расчетных центрах для осуществления клиринга;<br>• Периодическая оценка финансового состояния субъектов Системы и изменение лимитов по результатам;<br>• Осуществление расчетов в пределах, предоставленных |
| Риск потери ликвидности | • Риск потери ликвидности в большинстве случаев может быть следствием реализации Кредитного риска – исключение кредитного риска;<br>• Прогноз позиции денежных средств;<br>• Расчеты на нетто основе;<br>• Управление очередностью исполнения распоряжений Участников. |
| Общий коммерческий риск | • Организация и контроль системы принятия решений и делегирования полномочий;<br>• Организация и соблюдение внутренних управленческих правил и процедур, бизнес-процессов;<br>• Достижение планов по финансовому результату;<br>• Планирование расходов в соответствии с планами по финансовому результату;<br>• Применение мер по изменению стратегии в случае возникновения предпосылок по недостижению стратегических планов;<br>• Планирование инвестиций по поддержанию инфраструктуры Системы с обеспечением высокого уровня отказоустойчивости;<br>• Планирование инвестиций в квалифицированный персонал, обеспечивающий высокий уровень поддержки оказания УПИ;<br>• Сохранение высокого уровня деловой репутации. |

Перечень бизнес-процессов в Платежной Системе

| **Перечень бизнес-процессов Платежной Системы** | **Код бизнес-процесса** |
|---|---|
| Выполнение регуляторных требований | P1 |
| Клиентская поддержка | P2 |
| Мониторинг и управление рисками | P3 |
| Обеспечение доступности инфраструктуры Системы | P4 |
| Обеспечение офисной инфраструктуры организации | P5 |
| Операционные услуги | P6 |
| Расчетные услуги | P7 |
| Услуга платежного клиринга | P8 |
| Расширение каналов доступности услуги | P9 |
| Реализация бизнес-стратегии | P10 |

Содержание профиля значимого для Системы риска (в соответствии со Стандартом) — описание риск-событий, выявленных с применением не менее одного метода из числа, предусмотренных таблицей А.2 приложения А ГОСТ Р 58771-2019; выбранные методы фиксируются в профиле риска;

- описание причины возникновения каждого из риск-событий;
- описание бизнес-процессов, в которых могут произойти риск-события;
- вероятность наступления риск-событий, определённая с применением не менее одного метода, предусмотренного ГОСТ Р 58771-2019;
- описание и оценка неблагоприятных последствий каждого риск-события, выполненные методами из ГОСТ Р 58771-2019 с учётом результатов анализа сведений об инцидентах в Системе.
- описание бизнес-процессов и перечень субъектов Платежной Системы, на которые влияет риск-событие;
- уровень присущего риска до применения Способов управления рисками в Системе;
- уровень допустимого риска;
- уровень остаточного риска после применения Способов управления рисками;
- перечень Способов управления рисками в Системе.

Профиль риска нарушения БФПС должен составляться как сводный профиль в отношении всех значимых рисков в Системе, указанных в абзаце четвертом подпункта 2.2.4.2 пункта 2.2 Положения Банка России от 22 декабря 2017 года № 607-П.

Приложение № 5 к
Правилам платежной системы
«Система банковской кооперации» (версия 3.5)

# РЕГЛАМЕНТ СЭДО ПС СБК

## ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

**ПС СБК** – платежная система «Система банковской кооперации», оператором которой является ООО «Оператор банковской кооперации».

**Операционный Центр (ОЦ)** - общество с ограниченной ответственностью «БПЦ Процессинг», выполняющее функции операционного центра ПС СБК по договору с ООО «Оператор банковской кооперации».

**СЭДО ПС СБК (СЭДО)** – система электронного документооборота, организованная ОЦ, для обеспечения защищённого обмена информацией, необходимого для функционирования ПС СБК.

**Участник СЭДО (Участник)** - субъект ПС СБК (оператор ПС СБК, операторы услуг платежной инфраструктуры ПС СБК, в том числе ОЦ, банки - участники ПС СБК).

**Электронный документ (ЭД)** – документ, в котором информация представлена в электронно-цифровой форме.

**Электронная подпись (ЭП)** - информация в электронной форме, которая присоединена к электронному документу, использующаяся для однозначного подтверждения авторства и подлинности электронного документа, а также позволяющая установить факт изменения подписанного электронного документа после момента его подписания.

**Средства ЭП** - шифровальные (криптографические) средства, используемые для создания электронной подписи, проверки электронной подписи, создания ключа электронной подписи и ключа проверки электронной подписи.

**Средства шифрования** - аппаратные, программные и программно-аппаратные шифровальные (криптографические) средства, реализующие алгоритмы криптографического преобразования информации для ограничения доступа к ней, в том числе при ее хранении, обработке и передаче в Системе.

**Средства криптографической защиты информации (СКЗИ)** – средства электронной подписи и средства шифрования.

**Сертификат ключа проверки ЭП (самоподписанный сертификат, сертификат)** - электронный документ или документ на бумажном носителе, подтверждающие принадлежность ключа проверки электронной подписи Участнику.

**Ключ ЭП** – конфиденциальная уникальная последовательность символов известная только Участнику, сформировавшему данную последовательность, предназначенная для создания ЭП в ЭД.

**Ключ проверки ЭП** - уникальная последовательность символов, однозначно связанная с ключом ЭП и предназначенная для проверки ЭП.

**Участник, владелец ключа проверки ЭП** - Участник, который в установленном настоящим Регламентом порядке сформировал сертификат ключа проверки ЭП.

## 1. ОБЩИЕ ПОЛОЖЕНИЯ.

1.1. Настоящий Регламент регулируется Гражданским Кодексом Российской Федерации, Федеральным законом Российской Федерации от 06.04.2011 №63-ФЗ «Об электронной подписи», а также иными нормативными правовыми актами РФ. Регламент устанавливает порядок функционирования и использования СЭДО ПС СБК и обязателен для всех субъектов ПС СБК – Участников СЭДО.

СЭДО ПС СБК является основным каналом обмена документами между Субъектами Системы. Электронная почта и бумажные документы используются как резервные каналы в случаях, предусмотренных настоящим Регламентом и п. 1.5.2 Правил.

1.2. Участник признаёт, что

- любой ЭД, передаваемый посредством СЭДО, должен быть подписан ЭП Участника, инициирующего передачу ЭД в СЭДО, и зашифрован с использованием Сертификата ключа проверки ЭП (далее – Сертификата) принимающего Участника;

- ЭП в ЭД, сформированная с использованием Ключа ЭП, Сертификата и Средств ЭП, является равнозначной собственноручной подписи уполномоченного лица Участника- отправителя и оттиску печати Участника-отправителя при выполнении условий, определенных настоящим Регламентом. Наличие ЭП является необходимым и достаточным условием, позволяющим установить, что ЭД исходит от Участника, его отправившего (авторство документа), и гарантирует его неизменность (целостность документа);

- ЭД, подписанный подлинной ЭП Участника, юридически эквивалентен идентичному по содержанию документу на бумажном носителе, подписанному собственноручной подписью уполномоченного лица, скрепленному печатью данного Участника, и порождает для Участников аналогичные права и обязанности;

- использование в СЭДО Средств криптографической защиты информации (далее – СКЗИ), которые реализуют шифрование (Средства шифрования) и ЭП (Средства ЭП) ЭД, циркулирующих в Системе, достаточно для обеспечения конфиденциальности, подтверждения авторства, подлинности и целостности ЭД, передаваемых с помощью СЭДО;

- использование ЭД, подписанных ЭП, не изменяет содержания установленных прав и обязанностей Участников, содержания документов и правил заполнения их реквизитов, установленных договорами.

1.3. Участник обязуется

- принимать к исполнению ЭД, подписанные ЭП, для выполнения своих обязанностей в ПС СБК;

- хранить архивы входящих и исходящих ЭД, подписанных ЭП Участников, и квитанций о приеме ЭД в течение пяти лет с даты их отправки/получения;

- обеспечить хранение и конфиденциальность своих ключей ЭП и сертификатов Участников в течение шести лет с даты их формирования;

- обеспечить хранение использовавшихся для ЭДО Средств ЭП и Средств шифрования (дистрибутивов версий программного обеспечения), которые применялись для ЭП и шифрования ЭД в СЭДО в течение трех лет с даты их последнего использования в СЭДО в рамках настоящего Регламента.

1.4. Каждый Участник может иметь неограниченное число ключей ЭП и Сертификатов. При этом области применения Сертификатов для подписи различных типов ЭД могут различаться.

1.5. Риски, связанные с неправомерным подписанием ЭД ЭП, несет Участник – владелец соответствующего Сертификата ключа проверки ЭП.

## 2. СРЕДСТВА ЭЛЕКТРОННОЙ ПОДПИСИ.

2.1. Участник согласен:

- использовать в качестве Средств ЭП и шифрования СКЗИ «КриптоПро CSP» версии 4.0 или выше, приложение командной строки «cryptcp», разработанные ООО «КРИПТО-ПРО», а также «КриптоАРМ 5» разработанное ООО «Цифровые технологии»;

- эксплуатировать перечисленные Средства ЭП и шифрования в соответствии эксплуатационной документацией данных Средств.

2.2. Закупка необходимого числа лицензий на СКЗИ осуществляется Участником самостоятельно.

2.3. Участник признаёт, что

- ЭП, сформированная Средствами ЭП и применяемая в СЭДО в рамках настоящего Регламента, соответствует всем признакам и требованиям, предъявляемым к усиленной неквалифицированной ЭП, и предусмотренным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи»;

- используемые в СЭДО Средства ЭП:

- достаточны для подтверждения авторства и подлинности ЭД;
- позволяют установить факт изменения подписанного ЭД после его подписания;
- обеспечивают практическую невозможность вычисления ключа ЭП из значения самой ЭП или из ключа проверки ЭП.

## 3. СЕРТИФИКАТЫ КЛЮЧЕЙ ПРОВЕРКИ ЭЛЕКТРОННОЙ ПОДПИСИ.

3.1. Участник обязуется использовать, принимать и признавать Сертификаты ключей проверки ЭП, изданные другими Участниками.

3.2. Участник самостоятельно генерирует необходимое количество ключей ЭП, выпускает Сертификаты ключей проверки ЭП, после чего передает указанные Сертификаты другим Участникам.

3.3. При первичном обмене Сертификатами, а также в случае необходимости проведения внеплановой смены ключей ЭП, Участники обмениваются самоподписанными Сертификатами в электронном виде (формат x509 PEM) по электронной почте, с составлением Акта признания открытых ключей (Приложение 2 к настоящему Регламенту), подписанным уполномоченными лицами Участников и заверенным печатями.

3.4. При плановой смене ключей ЭП и Сертификатов Участники соглашаются передавать самоподписанные Сертификаты в электронном виде (формат x509 PEM) посредством СЭДО с обязательным их подписанием ключом ЭП Участника, Сертификат которого действует на момент передачи Сертификата, и шифрованием с использованием действующего Сертификата Участника-получателя. При завершении плановой смены Участник-инициатор плановой смены в течение 1 рабочего дня направляет в адрес противоположного Участника Акт признания открытого ключа (Приложение 2 к настоящему Регламенту). Акт признания открытого ключа оформляется на бумажном носителе, подписывается уполномоченным лицом Участника-инициатора и заверяется печатью.

3.5. Участник принимает, что идентификационные данные, занесенные в соответствующее поле Сертификата, однозначно идентифицируют Участника - владельца Сертификата, а также соответствуют его идентификационным данным.

3.6. Участник согласен, что область использования Сертификата, занесенная в соответствующее поле Сертификата, однозначно определяет область использования данного Сертификата в рамках реализации взаимоотношений между Участниками.

## 4. УСЛОВИЯ РАВНОЗНАЧНОСТИ ЭЛЕКТРОННОЙ ПОДПИСИ И СОБСТВЕННОРУЧНОЙ ПОДПИСИ.

ЭП в электронном документе признается подлинной и равнозначной собственноручной подписи уполномоченного лица Участника - владельца Сертификата, с использованием которого была создана ЭП, при одновременном соблюдении следующих условий:

- Сертификат является доверенным (то есть полученным Участником от уполномоченного лица другого Участника с составлением Акта признания

открытых ключей или полученным по СЭДО в виде ЭД, подписанного подлинной ЭП уполномоченного лица Участника-отправителя);

- Сертификат, относящийся к этой ЭП, не был отозван Участником-отправителем на момент получения ЭД Участником-получателем;

- Период действия Сертификата, относящийся к этой ЭП начался и не закончился на момент получения ЭД Участником-получателем;

- ЭП используется в соответствии с областью применения Сертификата, указанной в соответствующем поле Сертификата;

- Тип ЭД, подписанного ЭП, соответствует разрешенному типу документов в соответствии с областью применения Сертификата, указанной в соответствующем поле Сертификата;

- Проверка корректности ЭП с использованием Сертификата ключа проверки ЭП и Средства ЭП дает положительный результат.

## 5. СМЕНА КРИПТОГРАФИЧЕСКИХ КЛЮЧЕЙ И СЕРТИФИКАТОВ КЛЮЧЕЙ ПРОВЕРКИ ЭП.

5.1. Проведение Участником плановой смены своих криптографических ключей и Сертификатов является обязательным условием эксплуатации СЭДО. Срок действия криптографических ключей и Сертификатов составляет 12 (двенадцать) месяцев.

5.2. Участник самостоятельно и заблаговременно, не позднее, чем за 2 недели до момента окончания срока действия, генерирует новые криптографические ключи, формирует новые самоподписанные Сертификаты и направляет их в адрес других Участников в виде ЭД, подписанных действующим ключом ЭП и зашифрованных с использованием Сертификата принимающего Участника.

5.3. Внеплановая смена криптографических ключей производится в случае компрометации ключевой информации или истечения срока действия соответствующего Сертификата. При внеплановой смене криптографических ключей и Сертификата, Участник-инициатор внеплановой смены предоставляет другим Участникам новый самоподписанный Сертификат в электронном виде и оформляет новый Акт признания открытого ключа (Приложение 2 к настоящему Регламенту).

## 6. ДЕЙСТВИЯ В СЛУЧАЕ КОМПРОМЕТАЦИИ КЛЮЧЕВОЙ ИНФОРМАЦИИ.

6.1. К событиям, свидетельствующим о компрометации ключевой информации, относятся, в частности, следующие события:

- утрата ключевого носителя (в том числе с последующим обнаружением);
- возникновение подозрений на утечку информации или ее искажение в Системе;
- нарушение печати на сейфе с ключевыми носителями;
- нарушение безопасности компьютера (сервера), к которому был подключен ключевой носитель;

- доступ неуполномоченных лиц к Ключу ЭП, либо ключевому носителю (в том числе предполагаемый);
- иные обстоятельства, свидетельствующие прямо или косвенно о наличии возможности доступа к Ключу ЭП, либо ключевому носителю неуполномоченных лиц.

6.2. В случае компрометации ключа ЭП Участник - владелец соответствующего Сертификата обязан прекратить электронное взаимодействие в рамках СЭДО с использованием скомпрометированного ключа ЭП, незамедлительно известить ОЦ о факте компрометации и необходимости удаления из СЭДО Сертификата скомпрометированного ключа ЭП по телефону и электронной почте.

6.3. Не позднее 3 (трех) рабочих дней с момента компрометации ключевой информации Участник, ключ ЭП которого был скомпрометирован, обязан предоставить ОЦ письменное уведомление (Приложение 3 к Регламенту).

6.4. Участник, получивший уведомление о компрометации ключа ЭП от другого Участника, обязан не позднее 1 часа с момента получения уведомления удалить Сертификат скомпрометированного ключа из Системы и прекратить прием ЭД, подписанных скомпрометированным ключом ЭП.

6.5. Участник, ключ ЭП которого был скомпрометирован, организует и незамедлительно проводит внеплановую смену ключевой информации.

## 7. ОБЯЗАННОСТИ УЧАСТНИКА СЭДО.

7.1. Соблюдать правила работы в СЭДО, предусмотренные настоящим Регламентом и требованиями эксплуатационной документации на используемые СКЗИ.

7.2. Обеспечивать конфиденциальность своих ключей ЭП.

7.3. Немедленно прекратить использование ключа ЭП в случае его компрометации, незамедлительно уведомить о данном факте ОЦ и других Участников с целью предотвращения исполнения ЭД, подписанных скомпрометированным ключом.

7.4. Содержать в исправном состоянии программно-технические средства, применяемые для работы в СЭДО, принимать организационные и технические меры для предотвращения несанкционированного доступа к данным средствам и СКЗИ, а также в помещения, в которых они установлены.

7.5. Не допускать появления в среде функционирования программных средств СЭДО и СКЗИ компьютерных вирусов и иных вредоносных программ, несанкционированного доступа к ней неуполномоченных лиц.

7.6. Немедленно сообщать ОЦ обо всех случаях, свидетельствующих о попытках несанкционированного доступа к компьютерам (рабочим станциям и серверам) с установленными компонентами СЭДО и СКЗИ.

## 8. ОТВЕТСТВЕННОСТЬ.

8.1. Участник несёт ответственность за:

- неисполнение или ненадлежащее исполнение обязательств по настоящему Регламенту в рамках документально подтвержденного реального ущерба;
- содержание любых ЭД, подписанных его ЭП, если проверка ЭП, производимая в соответствии с настоящим Регламентом, дает положительный результат.

8.2. Участник освобождается от ответственности за убытки, причиненные другому Участнику, если ЭД, переданный другим Участником, не принят к исполнению получившим его Участником по причине невыполнения условий равнозначности ЭП собственноручной подписи, указанных в настоящем Регламенте.

8.3. При использовании телекоммуникационных каналов связи, принадлежащих организациям, предоставляющим услуги связи, Участник не несёт ответственности за возможные временные задержки при доставке ЭД, произошедшие не по его вине.

8.4. Участник не отвечает за неисполнение или ненадлежащее выполнение своих обязательств по настоящему Регламенту, если это было вызвано действиями (бездействием) другого Участника.

8.5. Ни один Участник не несет ответственность за нарушения работы СЭДО, вызванные техническими неполадками в работе оборудования и программного обеспечения других Участников, помехами в сетях связи, повреждениями линий связи, а также вызванные проникновением в компьютерные системы других Участников вредоносного ПО, фактами несанкционированного доступа к компьютерным системам других Участников, а также иными не зависящими от Участника причинами.

8.6. В случае прекращения действия настоящего Регламента Участник продолжает нести ответственность за электронные документы, созданные и исполненные в период действия настоящего Регламента.

## 9. РАЗРЕШЕНИЕ СПОРОВ

9.1. Все споры и разногласия, возникшие между Участниками в рамках настоящего Регламента, решаются путем переговоров.

9.2. В случае невозможности урегулирования возникших споров и разногласий путём переговоров создаётся Согласительная комиссия. Порядок работы Комиссии определён в Приложении 5 к настоящему Регламенту.

9.3. В случае невозможности урегулирования возникших споров, разногласий или требований путем переговоров, а также несогласия одной из Сторон с результатами работы Комиссии, возникшие между Сторонами споры, разногласия и претензии подлежат разрешению в Арбитражном суде города Москвы.

## 10. ОБСТОЯТЕЛЬСТВА НЕПРЕОДОЛИМОЙ СИЛЫ.

10.1. Участник освобождается от ответственности за частичное или полное неисполнение обязательств по настоящему Регламенту, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникших в результате обстоятельств чрезвычайного характера, которые невозможно было предвидеть или предотвратить никакими разумными мерами и способами.

10.2. Обстоятельствами чрезвычайного характера являются стихийные бедствия, аварии, пожары, техногенные катастрофы, произошедшие не по вине Участника; нормативные и

ненормативные акты органов власти и управления, а также их действия или бездействие, препятствующие выполнению Участником настоящего Регламента; забастовки, массовые беспорядки, военные действия, террористические акты, противоправные действия третьих лиц и другие обстоятельства, которые выходят за рамки разумного контроля Участника.

10.3. При наступлении обстоятельств, указанных в п. 10.2 настоящего Регламента, Участник, ссылающийся на возникновение обстоятельств непреодолимой силы, обязан известить о них ОЦ и других Участников в срок не позднее 10 (Десяти) рабочих дней и направить официальные документы, подтверждающие наличие этих обстоятельств. Извещение должно содержать данные о характере обстоятельств, а также оценку их влияния на возможность исполнения Участником своих обязательств по Регламенту и предполагаемый срок исполнения обязательств.

10.4. Если Участник не направит или несвоевременно направит извещение, предусмотренное п. 10.3 настоящего Регламента, то он обязан возместить другим Участникам понесенные ими убытки в согласованный срок.

10.5. Участник, ссылавшийся на возникновение обстоятельств, предусмотренных п. 10.2 настоящего Регламента, обязан известить ОЦ и других Участников о прекращении действий указанных обстоятельств в письменном виде не позднее 3 (Трех) календарных дней с даты их прекращения. В извещении должны быть указаны дата, с которой Участник возобновит выполнение своих функций по настоящему Регламенту, и срок, в течение которого Участник исполнит свои обязательства.

10.6. Если наступившие обстоятельства, перечисленные в п.10.2 настоящего Регламента, и их последствия продолжают действовать более двух месяцев, Участник и ОЦ проводят переговоры для выявления приемлемых альтернативных способов исполнения настоящего Регламента.

## 11. СРОК ДЕЙСТВИЯ РЕГЛАМЕНТА.

Настоящий Регламент действует без ограничения по времени, вступает в силу и становится обязательным для всех Участников с момента присоединения к ПС СБК до момента прекращения участия в ПС СБК.

## 12. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.

Все изменения и дополнения к настоящему Регламенту (Приложение № 5 к Правилам) вносятся в порядке п. 1.2 Правил и утверждаются Оператором. Операционный центр согласует изменения в части технической реализации обмена и СКЗИ, что оформляется актом согласования; согласование ОЦ не изменяет установленную Правилами процедуру утверждения.

Все приложения и дополнения к настоящему Регламенту являются его неотъемлемыми частями. Прекращение действия настоящего Регламента не влияет на статус электронных документов, которыми Участники обменивались в период действия Регламента.

Приложение 1
к Регламенту СЭДО ПС СБК

# ПОРЯДОК ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

Настоящее Приложение является неотъемлемой частью Регламента и определяет порядок электронного документооборота между Участниками.

## ОРГАНИЗАЦИЯ РАБОТЫ СИСТЕМЫ ЭЛЕКТРОННОГО ДОКУМЕНТООБОРОТА

1.1. Участники используют для обмена электронными документами существующие между ними технические каналы связи. Передача информации осуществляется посредством шифрованных VPN-туннелей между сетевым оборудованием Участников.

1.2. Для обмена электронными документами ОЦ организует сервер файлового обмена. Сервер файлового обмена ОЦ доступен для подключений со стороны Участников.

1.3. Сервер файлового обмена реализован на базе программного обеспечения OpenSSH (http://www.openssh.com/) и работает по протоколу SFTP (SSH File Transfer Protocol).

1.4. Для доступа на сервер файлового обмена Участник генерирует открытый и закрытый ключи алгоритма RSA длиной 2048, 3072 или 4096 бит и для аутентификации по протоколу SSH и передает ОЦ открытый ключ SSH. В качестве имён пользователей используются индивидуальные коды Участников ПС СБК, присвоенные Оператором ПС СБК (п. 2.8 Правил ПС СБК). Имена Оператора и ОЦ ПС СБК – «00» и «01», соответственно. Иным операторам услуг платежной инфраструктуры ПС СБК присваиваются имена пользователей в диапазоне 11-99. Обмен информацией (реквизитами доступа), указанной в настоящем подпункте, происходит по адресам электронной почты, указанным ОЦ и Участником, и подтверждается по другому каналу связи (телефон, бумажная почта).

1.5. Участник загружает файлы, содержащие ЭД, на сервер файлового обмена ОЦ в каталог: «/sftp/home/[имя_пользователя]/in», где «[имя_пользователя]» соответствует имени пользователя, предоставленному Участнику согласно подпункта 1.4. Имя каждого файла содержит только буквы латинского алфавита, цифры и следующие символы: - («минус»), _ («подчеркивание»), . («точка»). Имена файлов образуются по следующему шаблону: F «имя пользователя-отправителя»_«имя_пользователя-получателя»_«произвольный идентификатор»«.sig.enc» (исключая кавычки).

1.6. ОЦ размещает файлы, содержащие ЭД, предназначенные Участнику, на сервер файлового обмена ОЦ в каталоге: «/sftp/home/[имя_пользователя]/out», где «[имя_пользователя]» соответствует имени пользователя, полученному согласно подпункта 1.4.

1.7. Участники принимают друг от друга только файлы, загруженные согласно подпунктам 1.5 и 1.6 настоящего документа.

1.8. Участники подключаются к серверу файлового обмена ОЦ не реже, чем один раз в 10 минут и выгружают (получают) файлы из каталогов, указанных в п. 1.5 (выгружает ОЦ) и п. 1.6 (выгружает Участник). Сторона, выгрузившая (получившая) файл с ЭД, удаляет его с сервера файлового обмена ОЦ.

1.9. Размер каждого файла с ЭД не превышает 256 Мб (Двести пятьдесят шесть мегабайт, что эквивалентно 268’435’456 байтам).

## ПОРЯДОК ФОРМИРОВАНИЯ И ОБРАБОТКИ ЭД, ИХ ЭП И ШИФРОВАНИЯ

2.1. Участник-отправитель ЭД, после формирования содержимого ЭД перед его загрузкой на сервер файлового обмена ОЦ осуществляет подписание ЭД своей ЭП и последующее шифрование с использованием Сертификата Участника-получателя. ЭП используется с учетом указанных в Сертификате отправителя ограничений области применения и типа ЭД (перечень ЭД определен в Приложении 4 к настоящему Регламенту).

2.2. Участник-получатель, в случае получения в свой адрес ЭД формирует отчет о получении ЭД (Квитанцию (формат квитанции приведен в Приложении 4 к настоящему Регламенту)). В квитанции указывается наименование полученного ЭД и результат проверки ЭП Стороны-отправителя.

2.3. Квитанция подписывается ЭП Участника-получателя ЭД и направляется посредством СЭДО в адрес Участника-отправителя ЭД.

2.4. Событие получения Участником-отправителем квитанции с подтверждением положительного результата проверки ЭП исходящего ЭД и положительного результата проверки ЭП квитанции, сформированной Участником-получателем, является подтверждением факта получения и приема в обработку Участником-получателем исходящего ЭД.

2.5. В случае, если Участником-отправителем получена квитанция с отрицательным результатом проверки ЭП отправителя в переданном в адрес Участника-получателя ЭД, исходящий ЭД считается непринятым в обработку Участником-получателем.

2.6. В случае, если в течение 15 минут с момента отправки ЭД Участник-отправитель не получил квитанцию о его приеме Участником-получателем, либо результат проверки ЭП квитанции дал отрицательный результат, Участник-отправитель связывается с Участником-получателем с целью выяснения текущей ситуации, подтверждения приема/неприема ЭД в обработку, повторной отправки квитанции. Если ЭД не получен Участником-получателем, он отправляется повторно.

2.7. Прием в обработку полученных Участником-получателем ЭД производится только в случае успешности операций проверки Участником-получателем ЭП Участника-отправителя и расшифрования ЭД. Проверка ЭП осуществляется с использованием действующих на момент получения ЭД Сертификатов Участника-отправителя. Расшифрование ЭД производится Участником-получателем с использованием собственного ключа ЭП.

2.8. В случае направления Участником-отправителем неверно сформированного (ошибочного) ЭД представитель Участника-отправителя незамедлительно уведомляет Участника-получателя о неверно сформированном ЭД по телефону и электронной почте, сообщает время, дату, наименование ошибочного документа.

2.9. При получении уведомления об ошибочном ЭД, представитель Участника-получателя предпринимает меры для прекращения его обработки и отмены произведенных на его основании изменений, уведомляет о результатах представителя Участника-отправителя.

2.10. После получения от представителя Участника-получателя подтверждения об отмене неверно сформированного (ошибочного) ЭД, представитель Участника-отправителя формирует новый ЭД, подписывает его своей ЭП и направляет в адрес Участника-получателя посредством СЭДО.

2.11. Не позднее следующего рабочего дня с момента выявления неверно сформированного (ошибочного) ЭД, Участник-отправитель направляет в адрес Участника-получателя документ на бумажном носителе с подписью и печатью уполномоченного лица Стороны с указанием даты, времени, и идентификационных данных неверно сформированного ЭД и объяснением причины неверно сформированного ЭД.

2.12. Участники осуществляют ЭП ЭД в соответствии со стандартами ГОСТ Р 34.11-2012 «Информационная технология. Криптографическая защита информации. Функция хэширования» и ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи».

2.13. Участники осуществляют шифрование и имитозащиту ЭД в соответствии с ГОСТ 34.12-2018 «Системы обработки информации. Защита криптографическая».

Приложение 2
к Регламенту СЭДО ПС СБК

АКТ
признания открытого ключа _____

г. Москва «___» _____ 20___ г.

_____,
именуемый в дальнейшем «Участник 1», в лице _____,
действующего на основании _____, с одной стороны и
_____,
именуемый в дальнейшем «Участник 2», в лице _____,
действующего на основании _____, с
другой стороны, вместе именуемые Стороны, составили настоящий Акт признания открытого ключа _____ (далее - Акт) о нижеследующем:

1. Стороны признают открытый ключ, принадлежащий _____
Параметры ключа:
Окончание срока действия:
Начало срока действия:
Текст открытого ключа:

| |
|---|
| |

Дополнительные поля открытого ключа (средства проверки правильности ЭП):

| |
|---|
| Серийный номер ключа:<br>(CN):<br>(O):<br>Город (L):<br>Страна (C): RU<br>Адрес электронной почты (E):<br>Идентификатор ключа субъекта:<br>Отпечаток:<br>Данные об издателе:<br>Использование ключа: Цифровая подпись, Неотрекаемость, Шифрование данных, Согласование ключей, Подписывание сертификатов (dc) |

Ключ может использоваться в СЭДО для формирования ЭП в ЭД.

Ключ зарегистрирован и может использоваться для обмена ЭД в СЭДО с 00.00.00

«____» _____ 20__ г..

2. _____ предоставила сформированный открытый ключ (сертификат) _____.
3. Стороны по отношению друг к другу претензий не имеют.
4. Акт составлен в двух экземплярах, по одному экземпляру для каждой из Сторон.

| УЧАСТНИК 1: | УЧАСТНИК 2: |
| --- | --- |
| _____ | _____ |
| / / | / / |
| (подпись) | (подпись) |
| М.П. | М.П. |

Приложение 3
к Регламенту СЭДО ПС СБК

Уведомление
о факте компрометации закрытого ключа

г. Москва «___» _____ 20___ г.

_____(далее Участник 1), в лице _____, действующего на основании _____, уведомляет _____(далее Участник 2), о факте компрометации своего ключа ЭП по причине_____
_____
_____
_____:

Параметры ключа:
Окончание срока действия:
Начало срока действия:
Текст открытого ключа:

| |
|---|
| |

Дополнительные поля открытого ключа (средства проверки правильности ЭП):

| |
|---|
| Серийный номер ключа:<br>(CN):<br>(O):<br>Город (L):<br>Страна (C): RU<br>Адрес электронной почты (E):<br>Идентификатор ключа субъекта:<br>Отпечаток:<br>Данные об издателе:<br>Использование ключа: Цифровая подпись, Неотрекаемость, Шифрование данных, Согласование ключей, Подписывание сертификатов (dc) |

УЧАСТНИК 1:

_____
/ /
(подпись)

М.П.

УЧАСТНИК 2:

_____
/ /
(подпись)

М.П.

Приложение 4
к Регламенту СЭДО ПС СБК

Формат квитанций

Транспортная квитанция – подтверждение факта получения документа другой Стороной и корректность подписи)

- подтверждение получения файла и успешной проверки подписи:
{исходное имя файла}.{исходное расширение}.kv1.sig

- извещение об ошибке проверки подписи:
{исходное имя файла}.{исходное расширение}.er1.sig

Текст в файле-квитанции:
FILE: {исходное имя файла}.{исходное расширение}
HASH: {хэш по госту полученного файла *.sig.enc}
DATE_RECEIVE: {дата получения файла}
TIME_RECEIVE: {время получения файла}
STATUS: OK/ERROR, ({условный код ошибки}), {текст ошибки если есть}

Квитанция об обработке файла – подтверждение успешной загрузки данных в систему/обработки исполнителем и т.п.

- подтверждение успешной загрузки данных в систему/обработки исполнителем и т.п.
{исходное имя файла}.{исходное расширение}.kv2.sig

- извещение об ошибке загрузки данных в систему/ошибки обработки исполнителем и т.п.
{исходное имя файла}.{исходное расширение}.er2.sig

Текст в файле-квитанции:
FILE: {исходное имя файла}.{исходное расширение}
HASH: {хэш по госту полученного файла *.sig.enc}
DATE_PROCESSING: {дата обработки файла}
TIME_ PROCESSING: {время обработки файла}
STATUS: OK/ERROR, ({условный код ошибки}), {текст ошибки если есть}

Приложение 5
к Регламенту СЭДО ПС СБК

Порядок разрешения разногласий при обмене ЭД

1. Настоящий Порядок регулирует разрешение разногласий при обмене ЭД в рамках настоящего Регламента.

2. С целью разрешения разногласий при обмене ЭД, установления фактических обстоятельств, послуживших основанием их возникновения, а также для проверки целостности и подтверждения подлинности данных в ЭД создается Согласительная комиссия (далее - Комиссия).

3. Комиссия создается только при невозможности разрешить возникшую проблемную ситуацию в рамках переговоров Участников.

4. При возникновении разногласий при обмене ЭД, Участник, заявляющий о наличии разногласий (Участник-инициатор), обязан направить другому Участнику и ОЦ (или Оператору ПС СБК, если ОЦ является одной из Сторон разногласия) претензию, с подробным изложением причин разногласий и предложением организовать комиссию. Заявление должно содержать фамилии представителей Участника-инициатора, которые будут участвовать в работе комиссии, предложения по времени и дате начала работы комиссии (не позднее 7 дней со дня отправления заявления).

5. Комиссия собирается на территории Участника, к которому предъявляется претензия, при этом, указанный Участник должен письменно подтвердить свое согласие с предложением о дате и времени сбора комиссии либо предложить Участнику-инициатору другую дату и время сбора комиссии (не позднее 7 дней со дня получения заявления). Комиссия создается на срок до 14 дней.

6. В состав комиссии должно входить равное количество представителей каждого Участника, а также, представитель ОЦ (или Оператора ПС СБК, если ОЦ является одной из Сторон разногласия) и, в случае необходимости, независимые эксперты. Члены комиссии от каждого Участника назначаются приказами соответствующего Участника. В случае необходимости привлечения независимых экспертов эксперт считается назначенным только при согласии обоих Участников, выраженном в письменной форме. Порядок оплаты работы независимых экспертов в комиссии определяется по предварительному согласованию Сторон.

7. Стороны обязуются способствовать работе комиссии и не допускать отказа от предоставления необходимых документов и ознакомления с условиями и порядком работы своих программно-аппаратных средств, используемых для обмена ЭД.

8. По итогам работы комиссии составляется акт, который подписывается всеми членами комиссии.

9. Проверка фактов отправки и получения электронных документов производится путём анализа предоставленных комиссии Сторонами спорных электронных документов, Квитанций об их приеме, проверки корректности ЭП.

10. Процедуры проверки ЭП осуществляются на «чистом» от программного обеспечения компьютере, на который в присутствии членов комиссии устанавливается операционная

система, СКЗИ и программное обеспечение «КриптоАРМ» с эталонных носителей, полученных от производителей указанного программного обеспечения.

11. В случае, если Участник-инициатор утверждает, что не отправлял электронный документ, обработанный другим Участником, либо отправлял документ с иным содержимым:

Другой Участник предоставляет электронную копию подписанного ЭП Участника-инициатора спорного ЭД. Если спорный ЭД не был предоставлен другим Участником, спорная ситуация разрешается в пользу Участника-инициатора.

В ЭД, предъявленном другим Участником, проверяется корректность ЭП Участника-инициатора. Ключ проверки ЭП вводится вручную из оригинала Акта признания открытого ключа Участника-инициатора на бумажном носителе, подписанного уполномоченными представителями Сторон.

ЭП признается корректной в случае, если верно все из следующего:

- программное обеспечение «КриптоАРМ», установленное с эталонного диска, полученного от производителя данного программного обеспечения, дало положительный результат проверки ЭП;
- от Участника-инициатора не поступало информации о компрометации, либо подозрения на компрометацию ключей ЭП Участника-инициатора (подтверждения отправки таких уведомлений предоставляет другой Участник);
- на момент получения ЭД другим Участником, сертификат ключа проверки электронной подписи действовал (время получения ЭД берется из соответствующей Квитанции, отправленной другим Участником и снабженной ЭП другого Участника).

Если ЭП признается Комиссией некорректной, либо другой Участник не может предоставить Акт признания открытого ключа Участника-инициатора, который использовался при проверке ЭП, то спорная ситуация разрешается в пользу Участника-инициатора.

В остальных случаях спорная ситуация разрешается в пользу другого Участника.

Результаты работы Комиссии оформляются в виде Акта, который подписывается всеми членами Комиссии. По одному экземпляру Акта передается каждой Стороне, участвовавшей в работе Комиссии. Данный Акт в дальнейшем может использоваться Сторонами в качестве доказательства в суде.

Приложение № 6
к Правилам платежной системы
«Система банковской кооперации»
(версия 3.5)

# ПЛАН ДЕЙСТВИЙ, НАПРАВЛЕННЫХ НА ОБЕСПЕЧЕНИЕ НЕПРЕРЫВНОСТИ ДЕЯТЕЛЬНОСТИ И (ИЛИ) ВОССТАНОВЛЕНИЕ ДЕЯТЕЛЬНОСТИ (ПЛАН ОНиВД)

**Платежная система «Система банковской кооперации» (ПС «СБК»)**

Оператор: ООО «Оператор банковской кооперации»

| | |
|---|---|
| Версия документа | 1.0 |
| Дата | 15.02.2026 |
| Статус | Утверждён |
| Владелец документа | ООО «Оператор банковской кооперации» |
| Ответственный за актуализацию | Ответственный за СУР / БФПС |

## 1. Назначение и область применения

Настоящий План действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности (далее - План ОНиВД) определяет организационные и технологические меры, процедуры и порядок действий при возникновении нестандартных и чрезвычайных ситуаций, способных привести к приостановлению оказания услуг платежной инфраструктуры (УПИ) в ПС «СБК» либо к нарушению установленных уровней оказания УПИ.

План применяется Оператором ПС «СБК» и используется для координации взаимодействия с операторами услуг платежной инфраструктуры (ОУПИ) и участниками ПС «СБК» при реагировании на инциденты, влияющие на бесперебойность функционирования платежной системы (БФПС).

## 2. Нормативные и внутренние документы

План ОНиВД разработан на основании и с учетом требований и положений следующих документов:

- Федеральный закон от 27.06.2011 № 161-ФЗ «О национальной платежной системе».
- Положение Банка России от 22.12.2017 № 607-П «О требованиях к обеспечению бесперебойности функционирования платежной системы».
- Правила ПС «СБК» (версия 3.5) и приложения к ним.
- Порядок обеспечения БФПС в ПС «СБК» (Приложение № 4 к Правилам ПС «СБК», версия 3.5).
- Регламент СЭДО ПС «СБК» (Приложение № 5 к Правилам ПС «СБК», версия 3.5).

В части обмена сообщениями и документами при управлении инцидентами используются каналы связи, предусмотренные Правилами и Регламентом СЭДО: СЭДО - основной канал обмена электронными документами; электронная почта и документы на бумажных носителях - резервные каналы в предусмотренных случаях.

## 3. Термины и сокращения

- ОНиВД - обеспечение непрерывности деятельности и (или) восстановление деятельности.
- БФПС - бесперебойность функционирования платежной системы.
- УПИ - услуги платежной инфраструктуры (операционные, платежного клиринга и расчетные услуги).
- Оператор - ООО «Оператор банковской кооперации».
- ОУПИ - операторы услуг платежной инфраструктуры ПС «СБК».
- ОЦ - операционный центр ПС «СБК» (по Правилам/перечню ОУПИ).

- РЦ - расчетный центр ПС «СБК» (по Правилам/перечню ОУПИ).
- СЭДО - система электронного документооборота ПС «СБК».
- Инцидент БФПС - риск-событие, реализация которого привела или может привести к приостановлению (прекращению) оказания УПИ либо к нарушению установленных уровней оказания УПИ и (или) к иным неблагоприятным последствиям для БФПС.

## 4. Управление Планом: роли и ответственность

Управление Планом ОНиВД осуществляется в рамках распределенной модели управления рисками, установленной Правилами и Порядком обеспечения БФПС.

### 4.1. Исполнительный орган Оператора:

- утверждает План ОНиВД и изменения к нему;
- принимает решение об активации Плана ОНиВД, о переходе на резервный режим и о возврате в штатный режим;
- обеспечивает выделение ресурсов для реагирования и восстановления;
- рассматривает отчет по итогам инцидента и принимает решения о корректирующих мерах.

### 4.2. Ответственный за СУР/БФПС (управление рисками и БФПС)

- организует сбор и обработку сведений об инцидентах и показателях БФПС;
- координирует регистрацию инцидентов, оценку их влияния на БФПС и подготовку отчетных материалов;
- обеспечивает взаимодействие с ОУПИ и Участниками по вопросам БФПС (эскалация, получение подтверждений, контроль сроков восстановления);
- инициирует пересмотр Плана ОНиВД (не реже 1 раза в 2 года и по итогам значимых инцидентов/изменений).

### 4.3. Ответственный за информационную безопасность (ИБ)

- организует реагирование на инциденты ИБ, влияющие на оказание УПИ и/или на БФПС;
- обеспечивает взаимодействие с Участниками/ОУПИ по инцидентам ИБ в сроки, предусмотренные Правилами;
- инициирует ограничительные меры (при необходимости) для предотвращения дальнейшего ущерба.

### 4.4. Технический руководитель/ИТ (эксплуатация инфраструктуры Оператора)

- обеспечивает техническое выполнение переключения на резервный комплекс и (или) резервные сервисы поставщиков;
- организует восстановление данных и сервисов в пределах установленных сроков восстановления;
- ведет технические журналы и предоставляет артефакты для постинцидентного анализа.

**4.5. ОУПИ и Участники**
ОУПИ и Участники выполняют мероприятия по непрерывности и восстановлению в пределах своей зоны ответственности, предоставляют информацию Оператору и исполняют согласованные действия по переключению/восстановлению в сроки, установленные Правилами и Порядком обеспечения БФПС.

## 5. Основания активации Плана и уровни реагирования

План ОНиВД активируется при наступлении инцидента (или угрозы инцидента), который:

- привел или может привести к приостановлению (прекращению) оказания УПИ;
- привел или может привести к нарушению установленных уровней оказания УПИ;
- затрагивает критичные для функционирования ПС «СБК» сервисы, информационные системы или коммуникационные каналы.

Оператор устанавливает целевые сроки восстановления оказания УПИ и восстановления оказания УПИ в соответствии с требованиями к оказанию услуг:

- время восстановления услуг при приостановлении их оказания - не более 6 часов с момента нарушения УПИ;
- время восстановления в соответствии с требованиями к оказанию услуг - не более 72 часов с момента нарушения требований к оказанию услуг.

## 6. Порядок оповещения, эскалации и каналы связи

Оповещение и обмен информацией при реализации Плана ОНиВД осуществляется по согласованным каналам связи с учетом требований Правил и Регламента СЭДО.

Основной канал обмена электронными документами между Субъектами ПС «СБК» - СЭДО ПС «СБК». Резервные каналы - электронная почта и документы на бумажных носителях (в случаях, предусмотренных Регламентом СЭДО, включая форс-мажор).

Форма сбора контактных данных и матрица оповещения приведены в Приложении № 6.1 и Приложении № 6.2.

**6.1. Сроки информирования Оператора Участниками и ОУПИ (из Правил)**
Участники предоставляют Оператору информацию оперативно, в том числе:

- в случае возникновения обстоятельств, препятствующих оказанию услуг - незамедлительно в день возникновения;
- при выявлении чрезвычайных ситуаций/системных сбоев - незамедлительно;

- при выявлении инцидента защиты информации без финансовых последствий, затрагивающего технологические участки - не позднее 24 часов с момента возникновения (выявления), а также в течение 24 часов после устранения;
- при выявлении инцидента защиты информации, несущего финансовые последствия - незамедлительно, но не позднее 1 часа с момента выявления;
- при воздействии обстоятельств непреодолимой силы - в течение 1 рабочего дня (устно) и в течение 3 рабочих дней (письменно).

**6.2. Информирование Участников и Банка России Оператором**

Оператор информирует Банк России и Участников о случаях и причинах приостановления (прекращения) оказания УПИ в день такого приостановления (прекращения) в порядке, установленном Банком России, и с использованием согласованных каналов связи. Шаблоны сообщений приведены в Приложении № 6.2.

## 7. Мероприятия по обеспечению непрерывности и восстановлению

**7.1. Общий порядок реагирования на инцидент БФПС**

1) Регистрация события/инцидента и присвоение идентификатора (ID) инцидента; фиксация времени выявления.

2) Первичная классификация (тип инцидента, затронутые сервисы/УПИ, предполагаемая причина, предварительная оценка влияния на БФПС).

3) Эскалация руководителю Оператора и созыв кризисной группы (при необходимости).

4) Принятие решения об активации Плана ОНиВД и выборе сценария реагирования (переключение на резерв, переход на резервный сервис поставщика, ограничительные меры, иное).

5) Оповещение ОУПИ/Участников/Банка России (при применимости) в установленные сроки.

6) Выполнение технических и организационных мероприятий по восстановлению оказания УПИ.

7) Подтверждение восстановления, мониторинг стабильности и возврат в штатный режим.

8) Постинцидентный анализ и корректирующие мероприятия.

**7.2. Переход на резервный комплекс программных и технических средств**

При совмещении функций оператора платежной системы и платежно-клирингового центра Оператор обеспечивает возможность перехода на оказание УПИ через резервный комплекс программных и технических средств. Порядок переключения реализуется по чек-листам (Приложение № 6.4).

Резервный комплекс должен обеспечивать выполнение ключевых функций ПС «СБК» на уровне, достаточном для соблюдения установленных сроков восстановления (6 часов/72 часа). Технические параметры (режим резерва, RTO/RPO, состав систем) фиксируются в Приложении № 6.5 (подлежит заполнению и актуализации).

**7.3. Переход на резервные сервисы поставщиков услуг**

Оператор обеспечивает возможность перехода на использование резервных сервисов поставщиков услуг, если отказ основного сервиса может привести к приостановлению оказания УПИ. Критичные поставщики, сервисы и условия переключения фиксируются в Приложении № 6.5.

Порядок взаимодействия с поставщиками и подтверждение готовности резервных сервисов фиксируются в журнале инцидентов (Приложение № 6.3).

**7.4. Мероприятия при неработоспособности систем и сервисов поставщиков услуг**

В случае неработоспособности систем и сервисов поставщиков услуг нарушение предоставления которых способно привести к приостановлению оказания УПИ, Оператор:

- инициирует переключение на резервный сервис (если предусмотрено);
- при отсутствии резервного сервиса - активирует процедуру оперативного привлечения альтернативного поставщика и (или) временной замены функциональности;
- обеспечивает приоритетное восстановление критичных сервисов и коммуникаций;

Детализированные процедуры и контактные данные поставщиков закрепляются в Приложении № 6.1, Приложении № 6.4 и Приложении № 6.5 (подлежит заполнению).

**7.5. Инциденты защиты информации, влияющие на БФПС**

При инцидентах защиты информации (включая вредоносный код, компрометацию учетных данных, нарушения целостности/доступности), которые затрагивают оказание УПИ, Оператор и Субъекты Системы действуют в соответствии с Правилами и внутренними документами по ИБ, обеспечивая своевременное информирование и восстановление. Чек-листы реагирования приведены в Приложении № 6.4.

Сроки информирования по инцидентам ИБ со стороны Участников приведены в п. 6.1 настоящего Плана (не позднее 24 часов / не позднее 1 часа в зависимости от последствий).

**7.6. Форс-мажор и недоступность персонала/площадок**

При воздействии обстоятельств непреодолимой силы и иных событий, приводящих к недоступности персонала, площадок или коммуникаций, Оператор обеспечивает организацию удаленной работы (при наличии технической возможности), приоритизацию задач восстановления и использование резервных каналов связи. Уведомление Оператора о форс-мажоре осуществляется в сроки, указанные в п. 6.1.

**7.7. Взаимозаменяемость расчетных центров (при наличии нескольких РЦ)**

В целях восстановления оказания УПИ и обеспечения устойчивости расчетов участники должны иметь банковский счет не менее чем в двух расчетных центрах (при наличии

нескольких РЦ в ПС «СБК»). Механизм переключения расчетов, порядок уведомления и подтверждения готовности подлежат закреплению в регламенте и включены в реестр пробелов (Приложение № 6.6).

## 8. Восстановление и возврат в штатный режим

Возврат из резервного режима в штатный режим осуществляется по решению руководителя Оператора после подтверждения стабилизации и готовности основной инфраструктуры.

Минимальные условия возврата в штатный режим:

- восстановлено оказание УПИ и обеспечена устойчивость функционирования;
- проведены контрольные проверки (целостность данных, доступность ключевых сервисов, корректность обмена сообщениями);
- выполнено оповещение Участников (и при необходимости Банка России) о восстановлении.
- зафиксированы результаты и артефакты переключения (журналы, отчеты, временные параметры).

Чек-листы возврата приведены в Приложении № 6.4.

## 9. Постинцидентный анализ и корректирующие мероприятия

Оператор оценивает влияние каждого инцидента на БФПС не позднее рабочего дня, следующего за днем выявления инцидента, а также не позднее окончания рабочего дня, следующего за днем устранения последствий инцидента. Также проводится оценка влияния на БФПС всех инцидентов за календарный месяц в течение пяти рабочих дней после окончания месяца.

По итогам инцидента Ответственный за СУР/БФПС организует подготовку отчета (Приложение № 6.3) и анализ эффективности мероприятий по восстановлению. Результаты используются при управлении рисками и при пересмотре Плана ОНиВД.

## 10. Тестирование, учения, обучение и пересмотр

План ОНиВД подлежит проверке (тестированию) и пересмотру с периодичностью не реже одного раза в два года. Дополнительно План пересматривается по результатам значимых инцидентов и при существенных изменениях бизнес-процессов/инфраструктуры.

Форматы тестирования (table-top, технические переключения, восстановление из резервных копий), периодичность и ответственные лица подлежат определению и закреплению (см. Приложение № 6.6).

## 11. Хранение документов, журналы и конфиденциальность

Документы и артефакты, формируемые при реализации Плана ОНиВД (уведомления, журналы, отчеты, подтверждения переключения), хранятся Оператором в соответствии с требованиями Правил и Порядка обеспечения БФПС, но не менее 5 лет с даты получения/формирования, если иное не установлено законодательством.

Информация, содержащая сведения о средствах и методах обеспечения информационной безопасности, а также иная ограниченная информация, обрабатывается и хранится с соблюдением режимов конфиденциальности, установленных Правилами и законодательством Российской Федерации.

## 12. Приложения

Состав и формы приложений являются неотъемлемой частью настоящего Плана ОНиВД:

- Приложение № 6.1. Контакт-лист и каналы связи (кризисное управление).
- Приложение № 6.2. Матрица оповещения и шаблоны уведомлений (Участникам, ОУПИ, Банку России).
- Приложение № 6.3. Журнал регистрации инцидентов и форма постинцидентного отчета.
- Приложение № 6.4. Чек-листы по основным сценариям (переключение/возврат, отказ поставщика, ИБ-инцидент, форс-мажор).
- Приложение № 6.5. Перечень критичных процессов, сервисов и объектов инфраструктуры (BIA/инвентаризация) и целевые параметры восстановления.

**Приложение № 6.1**
к Плану ОНиВД (Приложение № 6 к Правилам ПС «СБК» версия 3.5)

## КОНТАКТ-ЛИСТ И КАНАЛЫ СВЯЗИ (КРИЗИСНОЕ УПРАВЛЕНИЕ)

Таблица подлежит заполнению и актуализации перед запуском платежной системы в эксплуатацию. Контактные данные должны включать как минимум основной и резервный каналы связи, а также режим доступности (24x7/в рабочее время).

| Роль/функция | Организация/подразделение | ФИО | Должность | Телефон (осн.) | Телефон (рез.) | Email | Примечание/канал (СЭДО, мессенджер и т.п.) |
|---|---|---|---|---|---|---|---|
| Руководитель Оператора | Оператор | [ФИО] | [должность] | [+7...] | [+7...] | [email] | Решение об активации Плана |
| Ответственный за СУР/БФПС | Оператор | [ФИО] | [должность] | [+7...] | [+7...] | [email] | Координация БФПС, учет инцидентов |
| Ответственный за ИБ | Оператор | [ФИО] | [должность] | [+7...] | [+7...] | [email] | Реагирование на ИБ-инциденты |
| ИТ/Эксплуатация (дежурная смена) | Оператор | [ФИО/группа] | [должность] | [+7...] | [+7...] | [email] | Технические переключения |
| Операционный центр (ОЦ) | ОУПИ | [организация] | [контакт] | [+7...] | [+7...] | [email] | Дежурный контакт ОЦ |
| Расчетный центр (РЦ) | ОУПИ | [организация] | [контакт] | [+7...] | [+7...] | [email] | Дежурный контакт РЦ |
| Банк России (контакт/канал) | Банк России | [подразделение] | [контакт] | [тел.] | [тел.] | [email/ЛК] | Канал информирования: [ЛК/иное] |

**Приложение № 6.2**
к Плану ОНиВД (Приложение № 6 к Правилам ПС «СБК» версия 3.5)

## МАТРИЦА ОПОВЕЩЕНИЯ И ШАБЛОНЫ УВЕДОМЛЕНИЙ

### 6.2.1. Матрица оповещения (эскалация)

| Событие/триггер | Кого уведомляем | Срок | Канал | Ответственный за отправку | Подтверждение получения |
|---|---|---|---|---|---|
| Приостановление (прекращение) оказания УПИ / существенный сбой | Банк России; Участники; ОУПИ | В день приостановления | СЭДО (осн.); email (рез.) | Ответственный за СУР/БФПС | Квитанция СЭДО / ответ email |
| Нарушение установленных уровней оказания УПИ | Участники; ОУПИ | Незамедлительно после подтверждения | СЭДО; телефон (при необходимости) | Ответственный за СУР/БФПС | Фиксация в журнале |
| ИБ-инцидент без фин. последствий (затрагивает технологические участки) | Оператор (ИБ); ОУПИ/Участники (если затронуты) | До 24 часов (по Правилам для Участников) | СЭДО; email | Ответственный за ИБ | Фиксация в журнале |
| ИБ-инцидент с фин. последствиями | Оператор (ИБ); ОУПИ/Участники (если затронуты) | Незамедлительно, но не позднее 1 часа (по Правилам для Участников) | Телефон + СЭДО | Ответственный за ИБ | Фиксация времени звонка |
| Форс-мажор | Оператор; ОУПИ/Участники | 1 рабочий день (устно) / 3 рабочих дня (письменно) | Телефон; СЭДО; бумага (при необходимости) | Ответственный за СУР/БФПС | Квитанция/акт |

### 6.2.2. Шаблон уведомления Участникам о приостановлении/нарушении УПИ

Тема: Уведомление об инциденте БФПС / приостановлении оказания УПИ в ПС «СБК»

ID инцидента: [SBK-YYYYMMDD-XXX]

Дата/время начала инцидента (МСК): [__]

Затронутые сервисы/УПИ: [__]

Описание/причина (предварительно): [__]

Оценка влияния: [приостановление/ухудшение уровня оказания УПИ], ожидаемое время восстановления: [__] (целевое значение - до 6 часов при приостановлении).

Принятые меры: [переключение на резерв/работы по восстановлению/ограничительные меры].

Следующее обновление статуса: [время].

Контакт для взаимодействия (24x7): [ФИО, тел., email].

Подпись: ООО «Оператор банковской кооперации».

**6.2.3. Шаблон уведомления Участникам о восстановлении**
Тема: Уведомление о восстановлении оказания УПИ / завершении инцидента БФПС в ПС «СБК»

ID инцидента: [SBK-YYYYMMDD-XXX]

Дата/время восстановления (МСК): [__]

Краткое описание выполненных работ: [__]

Статус: оказание УПИ восстановлено, система функционирует в штатном режиме.

Дополнительные рекомендации Участникам (при наличии): [__]

Контакт для обратной связи: [__].

Подпись: ООО «Оператор банковской кооперации».

**6.2.4. Шаблон уведомления Банку России**
Адресат: Банк России (в порядке и по каналу, установленным Банком России).

Тема: Информация о приостановлении (прекращении) оказания УПИ / инциденте БФПС в ПС «Система банковской кооперации» (рег. № 0046).

Дата/время начала инцидента (МСК): [__].

Описание инцидента и причины (предварительно): [__].

Затронутые услуги/элементы платежной инфраструктуры: [__].

Принятые меры (в т.ч. переключение на резервный комплекс/резервные сервисы поставщиков): [__].

Ожидаемые сроки восстановления: [__].

Контактное лицо: [ФИО, должность, телефон, email].

Приложения (при необходимости): [лог/отчет/иное].

Подпись: ООО «Оператор банковской кооперации».

**Приложение № 6.3**
к Плану ОНиВД (Приложение № 6 к Правилам ПС «СБК» версия 3.5)

## ЖУРНАЛ РЕГИСТРАЦИИ ИНЦИДЕНТОВ И ФОРМА ПОСТИНЦИДЕНТНОГО ОТЧЕТА

### 6.3.1. Журнал регистрации инцидентов (форма)

| ID | Дата/время начала (МСК) | Дата/время выявления (МСК) | Тип (УПИ/ИБ/поставщик/форс-мажор) | Затронутые сервисы/ УПИ | Краткое описание | Влияние на БФПС (да/нет) | Приостановление УПИ (да/нет) | Время восстановления (факт) | Сроки (6ч/72ч) соблюдены (да/нет) | Уведомления (Участники/БР) | Ответственный | Статус |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |
| | | | | | | | | | | | | |

### 6.3.2. Постинцидентный отчет (шаблон)

**ПОСТИНЦИДЕНТНЫЙ ОТЧЕТ**

1) ID инцидента: [__]

2) Дата/время начала (МСК): [__]

3) Дата/время выявления (МСК): [__]

4) Дата/время восстановления (МСК): [__]

5) Затронутые сервисы/УПИ: [__]

6) Описание причины (root cause): [__]

7) Оценка влияния на БФПС (финансовое/нефинансовое, клиенты/Участники/ОУПИ): [__]

8) Соблюдение сроков восстановления (6 часов/72 часа): [да/нет], комментарий: [__]

9) Выполненные мероприятия (по этапам): [__]

10) Коммуникации: кого уведомили, когда, по каким каналам; подтверждения: [__]

11) Уроки и корректирующие меры (CAPA): [__]

12) Необходимые изменения в План ОНиВД/регламенты/инфраструктуру: [__]

13) Ответственные и сроки выполнения корректирующих мер: [__]

14) Приложения (логи, скриншоты, акты, подтверждения): [__]

**Приложение № 6.4**
к Плану ОНиВД (Приложение № 6 к Правилам ПС «СБК» версия 3.5)

# ЧЕК-ЛИСТЫ ПО ОСНОВНЫМ СЦЕНАРИЯМ

### 6.4.1. Переключение на резервный комплекс (инициация и выполнение)

[ ] Зафиксировать ID инцидента, время начала и затронутые сервисы/УПИ.

[ ] Оценить необходимость активации Плана ОНиВД и переключения на резервный комплекс.

[ ] Согласовать решение с руководителем Оператора (если требуется).

[ ] Оповестить ОУПИ (ОЦ/РЦ) и Участников о работах/инциденте (по матрице оповещения).

[ ] Зафиксировать точку консистентности данных (если применимо), выполнить резервное копирование/снимок.

[ ] Выполнить переключение (DNS/маршрутизация/балансировщики/очереди сообщений - указать в runbook).

[ ] Проверить доступность ключевых функций и корректность обработки сообщений/переводов (контрольные операции).

[ ] Зафиксировать время восстановления и начать усиленный мониторинг (первые 60 минут).

[ ] Направить обновление статуса Участникам/ОУПИ/Банку России (при применимости).

### 6.4.2. Возврат с резервного комплекса на основной

[ ] Подтвердить готовность основного комплекса (результаты диагностики, устранение причины).

[ ] Согласовать окно переключения и уведомить заинтересованных лиц.

[ ] Синхронизировать данные/очереди/журналы (если применимо).

[ ] Выполнить переключение на основной комплекс по runbook.

[ ] Провести контрольные проверки целостности и корректности процессов.

[ ] Уведомить Участников о возврате в штатный режим.

[ ] Закрыть инцидент, оформить постинцидентный отчет.

**6.4.3. Отказ критичного поставщика услуг**

[ ] Определить сервис поставщика и зависимые процессы/УПИ.

[ ] Связаться с поставщиком, получить подтверждение статуса и прогноз восстановления.

[ ] При наличии резервного сервиса - инициировать переключение.

[ ] При отсутствии резерва - активировать временные меры (ручные процедуры/альтернативные каналы).

[ ] Уведомить Участников/ОУПИ о влиянии и предполагаемых сроках.

[ ] Зафиксировать договорные/регуляторные последствия (SLA, отчеты).

[ ] По восстановлении - выполнить проверку и оформить отчет.

**6.4.4. Инцидент информационной безопасности, влияющий на БФПС**

[ ] Инициировать реагирование ИБ (сбор данных, изоляция, ограничительные меры).

[ ] Оценить влияние на оказание УПИ и необходимость переключения на резервные мощности.

[ ] Обеспечить уведомление Оператора/ОУПИ/Участников в установленные сроки (в зависимости от последствий).

[ ] Восстановить работоспособность и провести проверку целостности данных.

[ ] Оформить отчет и корректирующие меры (обновление политик, обучение, технические меры).

**6.4.5. Форс-мажор/недоступность площадки или персонала**

[ ] Активировать резервные каналы связи и удаленный режим работы (если предусмотрено).

[ ] Определить состав доступных ключевых ролей и назначить заместителей.

[ ] Приоритизировать критичные функции ПС «СБК».

[ ] Организовать взаимодействие с ОУПИ и Участниками по альтернативным каналам.

[ ] Зафиксировать события и оформить уведомления в установленные сроки.

**Приложение № 6.5**
к Плану ОНиВД (Приложение № 6 к Правилам ПС «СБК» версия 3.5)

## КРИТИЧНЫЕ ПРОЦЕССЫ/СЕРВИСЫ И ЦЕЛЕВЫЕ ПАРАМЕТРЫ ВОССТАНОВЛЕНИЯ (ШАБЛОН)

Раздел подлежит заполнению на основании инвентаризации и анализа влияния на бизнес (BIA). Рекомендуется выделять как минимум: критичные УПИ, критичные ИС/компоненты, зависимости от ОУПИ и поставщиков, целевые RTO/RPO.

| Процесс/сервис | Описание/критичность | Владелец | Зависимые УПИ/участники | Ключевые системы/компоненты | Зависимости (ОУПИ/поставщики) | RTO (цель) | RPO (цель) | Резервный вариант/комментарий |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |