СООТВЕТСТВУЕТ

«14» ноября 2023 г.

УТВЕРЖДАЮ:
Заместитель Председателя Правления
ПАО Сбербанк

А.Л.Попов

«12» октября 2023 г.

ПРАВИЛА

ПЛАТЕЖНОЙ СИСТЕМЫ

«СБЕРБАНК»

Москва
2023

СОДЕРЖАНИЕ

Правила Платежной системы «Сбербанк», далее — Правила, разработаны Публичным акционерным обществом «Сбербанк России» (ПАО Сбербанк), далее - Оператор платежной системы, и регламентируют условия участия в Платежной системе «Сбербанк» (далее - Платежная система, ПС), осуществления перевода денежных средств, оказания услуг платежной инфраструктуры (далее также УПИ), права и обязанности Участников платежной системы и иные условия, определяемые Оператором платежной системы в соответствии с требованиями законодательства Российской Федерации.

Текст настоящих Правил публикуется на официальном сайте ПАО Сбербанк по адресу http://www.sberbank.ru/ru/credit org/bankingservice/corespondent relations.

1. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Банк - ПАО Сбербанк, Оператор платежной системы «Сбербанк»

Бизнес-процесс - процесс, в рамках которого обеспечивается оказание УПИ.

Договор банковского счета - Договор корреспондентского счета в валюте Российской Федерации или иностранной валюте, заключенный между ПАО Сбербанк и Участником платежной системы.

Обмен электронными сообщениями - получение/передача Оператором платежной системы электронных сообщений, содержащих распоряжения Участников платежной системы, а также извещений (подтверждений) о приеме и об исполнении распоряжений Участников платежной системы в рамках выполнения Оператором платежной системы функций операционного центра, платежного клирингового центра, расчетного центра.

Оператор платежной системы (Оператор) - организация, определяющая Правила, а также выполняющая иные обязанности, предусмотренные Федеральным законом от 27.06.2011 №161-ФЗ "О национальной платежной системе" (далее - Федеральный закон №161-ФЗ). Оператором ПС «Сбербанк» является ПАО Сбербанк.

Оператор по переводу денежных средств - организация, которая в соответствии с законодательством Российской Федерации вправе осуществлять перевод денежных средств.

Операционный центр - подразделение Оператора платежной системы, обеспечивающее в рамках Платежной системы для Участников платежной системы и их клиентов доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа, а также обмен электронными сообщениями (далее - операционные услуги).

Оператор услуг платежной инфраструктуры (Оператор УПИ) - операционный центр, платежный клиринговый центр и расчетный центр**.**

Перевод денежных средств - действия Оператора по переводу денежных средств в валюте Российской Федерации и иностранной валюте в рамках применяемых форм безналичных расчетов по предоставлению получателю денежных средств плательщика с использованием счетов Участников платежной системы, открытых у Оператора платежной системы, являющегося Расчетным центром платежной системы.

Платежная система - совокупность организаций, взаимодействующих по Правилам в целях осуществления перевода денежных средств, включающая Оператора платежной системы, операторов услуг платежной инфраструктуры и Участников платежной системы (совместно именуемых Стороны), из которых как минимум три участника являются Операторами по переводу денежных средств.

Платежный клиринговый центр - подразделение Оператора платежной системы, обеспечивающее в рамках Платежной системы прием к исполнению распоряжений Участников платежной системы об осуществлении перевода денежных средств и выполнение иных действий, предусмотренных Федеральным законом №161-ФЗ (далее - услуги платежного клиринга).

Правила платежной системы -документ (документы), содержащий (содержащие) условия участия в платежной системе, осуществления перевода денежных средств, оказания услуг платежной инфраструктуры и иные условия, определяемые Оператором платежной системы.

Расчетный центр - подразделение Оператора платежной системы, обеспечивающее в рамках Платежной системы исполнение распоряжений Участников платежной системы посредством списания и зачисления денежных средств по Счетам Участников платежной системы, а также направление подтверждений, касающихся исполнения распоряжений Участников платежной системы (далее - расчетные услуги).

Счет - корреспондентский счет Лоро в валюте Российской Федерации или иностранной валюте, открытый кредитной организацией у Оператора платежной системы «Сбербанк», по которому осуществляются операции по списанию и зачислению средств в соответствии с законодательством Российской Федерации и Договором банковского счета. В случае присоединения Оператора по переводу денежных средств к Правилам в качестве Участника платежной системы по Счету проводятся операции по переводу денежных средств в соответствии с законодательством Российской Федерации и Правилами.

Участники платежной системы (Участники) - Операторы по переводу денежных средств, открывшие корреспондентские счета у Оператора платежной системы, и присоединившиеся к Правилам в целях оказания Оператором услуг по переводу денежных средств между прямыми Участниками. Оператор является Участником платежной системы.

2. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ ПЛАТЕЖНОЙ СИСТЕМЫ

Наименование платежной системы - Платежная система «Сбербанк».

Оператор платежной системы «Сбербанк» - Публичное акционерное общество «Сбербанк России» (ПАО Сбербанк).
Регистрационный номер Банка России - Генеральная лицензия Банка России на осуществление банковских операций №1481 от 11.08.2015 г.

Юридический адрес:	Россия, Москва, 117997, ул. Вавилова, д. 19
Почтовый адрес;	Москва, 117997, ул. Вавилова, д. 19 (+7 495) 500-55-50, (8 800) 555-55-50
Справочная служба:	
Электронная почта:	sberbank@sberbank.ru
Сайт:	www.sberbank.ru, www.sberbank.com
Код SWIFT:	SABRRUMM

Реквизиты:

Корреспондентский счет	30101810400000000225 в Главном управлении Центрального банка Российской Федерации по Центральному федеральному округу г. Москва (ГУ Банка России по ЦФО)
БИК	044525225
ИНН:	7707083893
КПП	773601001

Email:

- по вопросам функционирования платежной системы «Сбербанк» и условиям Правил Платежной системы PS Sberbank@sberbank.ru,
- по вопросам защиты информации: spss@sberbank.ru.

3. ФУНКЦИИ И ПРАВА ОПЕРАТОРА ПЛАТЕЖНОЙ СИСТЕМЫ

3.1 Оператор платежной системы осуществляет свою деятельность по переводу денежных средств в соответствии с Федеральным законом от 27.06.2011 № 161-ФЗ «О национальной платежной системе» и нормативными актами Банка России.

3.2 Оператор платежной системы:

- определяет Правила Платежной системы, организует и осуществляет контроль за соблюдением Правил Участниками платежной системы,
- совмещает функции оператора услуг платежной инфраструктуры и обеспечивает контроль за оказанием услуг платежной инфраструктуры Участникам платежной системы,
- организует систему управления рисками в Платежной системе, осуществляет оценку и управление рисками в Платежной системе, обеспечивает бесперебойность функционирования Платежной системы в порядке, установленном Банком России;
- обеспечивает бесперебойность оказания услуг платежной инфраструктуры Участникам платежной системы;
- обеспечивает возможность досудебного и (или) третейского рассмотрения споров с Участниками платежной системы, в том числе, в рамках оказания услуг платежной инфраструктуры (УПИ), в соответствии с Правилами платежной системы.

3.3 Оператор платежной системы информирует о случаях и причинах приостановления (прекращения) оказания УПИ в день такого приостановления (прекращения):

- Банк России (Департамент национальной платежной системы, далее - ДНПС) посредством направления сообщения на бумажном носителе или электронного сообщения, снабженного кодом аутентификации, в течение двух рабочих дней со дня приостановления (прекращения) оказания УПИ. При этом Оператор платежной системы в день приостановления (прекращения) оказания УПИ незамедлительно направляет в Банк России (ДНПС) уведомление о приостановлении (прекращении) оказания УПИ с использованием способа связи, информация о котором доведена до него Банком России (ДНПС).
- Участников платежной системы путем направления уведомления с использованием способа связи, обеспечивающего оперативную доступность информации (размещение на официальном сайте, направление уведомления по электронной почте, иные способы).

3.4 Оператор платежной системы может взаимодействовать с другими платежными системами, перечень которых содержится в реестре операторов платежных систем, опубликованном на официальном сайте Банка России.

3.5 В случае возникновения необходимости взаимодействия с другим(и) оператором(ами) платежных систем Оператор платежной системы в порядке, предусмотренном разделом 19 настоящих Правил, вносит в Правила соответствующие изменения, касающиеся указания перечня платежных систем, с которыми осуществляется взаимодействие, определения порядка взаимодействия Оператора платежной системы с оператором другой платежной системы, а также форму заключаемого между ними договора о взаимодействии.

3.6 Информационное взаимодействие с внешними заинтересованными сторонами и компетентными органами в части, относящейся к функционированию платежной системы, осуществляется подразделением Банка, ответственным за организацию и развитие функционирования Платежной системы «Сбербанк».

4. ВИДЫ И КРИТЕРИИ УЧАСТИЯ, ПРЕКРАЩЕНИЕ УЧАСТИЯ В ПЛАТЕЖНОЙ СИСТЕМЕ

4.1 Правилами предусматривается только прямое участие в Платежной системе. Прямыми участниками платежной системы могут являться только Операторы по переводу денежных средств - резиденты при условии их присоединения к настоящим Правилам в целом.

4.2 Критерии участия Оператора по переводу денежных средств в Платежной системе определяются Оператором платежной системы. Участник платежной системы должен соответствовать следующим требованиям:

- Иметь необходимые лицензии на осуществление банковской деятельности.
- Обладать техническими средствами для обмена по системам дистанционного банковского обслуживания (ДБО[1]), другим каналам связи.

4.3 Участие оператора по переводу денежных средств в Платежной системе начинается после присоединения к Правилам при условии открытия Счета у Оператора платежной системы. Операторы по переводу денежных средств представляют Оператору платежной системы Договор присоединения по форме, установленной Приложением 1.

4.4 Приостановление участия в Платежной системе не применяется.

4.5 Участие Участника платежной системы в Платежной системе прекращается в следующих случаях:

- при несоответствии критериям, предусмотренным п.4.2 настоящих Правил;
- с даты прекращения действия всех Договоров банковского счета,
- после выхода (отказа от участия) Участника платежной системы из Платежной системы и расторжения Договора присоединения,
- в иных случаях, предусмотренных требованиями законодательства и/или Договором присоединения.

4.6 Оператор платежной системы имеет право запросить у Участников платежной системы информацию, подтверждающую соответствие критериям/требованиям участия (привлечения), а также соблюдение Правил платежной системы.

5. ПОРЯДОК ПРИСВОЕНИЯ КОДА (НОМЕРА), ПОЗВОЛЯЮЩЕГО ОДНОЗНАЧНО УСТАНОВИТЬ УЧАСТНИКА ПЛАТЕЖНОЙ СИСТЕМЫ И ПРИЗНАК ЕГО УЧАСТИЯ В ПЛАТЕЖНОЙ СИСТЕМЕ

5.1 Для идентификации Участника платежной системы используется уникальный идентификатор, который соответствует присвоенному Банком России Участнику платежной системы БИК, а также 20-значный номер счета, открытый Участнику платежной системы Оператором платежной системы.

5.2 При обмене электронными сообщениями в качестве идентификатора может использоваться международный банковский идентификационный код SWIFT BIC, а также 20-значный номер счета, открытого Участнику платежной системы Оператором платежной системы.

5.3 В нормативно-справочной информации (НСИ) Оператора платежной системы подразделениями, ответственными за открытие и сопровождение Счетов, с даты присоединения к Правилам платежной системы Участнику присваивается признак его участия в Платежной системе и указывается дата заключения Договора присоединения. Информация об Участнике, включая его статус в Платежной системе, вносится по месту открытия Счета. Признак аннулируется с даты исключения Участника из Платежной системы по основаниям,

[1] Приложение 5

предусмотренным п.4.5 Правил. Обновление и тиражирование НСИ осуществляется Оператором платежной системы ежедневно.

6. ПОРЯДОК ОБЕСПЕЧЕНИЯ ИСПОЛНЕНИЯ ОБЯЗАТЕЛЬСТВ УЧАСТНИКОВ ПЛАТЕЖНОЙ СИСТЕМЫ ПО ПЕРЕВОДУ ДЕНЕЖНЫХ СРЕДСТВ

6.1 Обеспечением исполнения обязательств Участников платежной системы по переводу денежных средств является достаточность денежных средств на Счетах Участников платежной системы. При недостаточности средств на Счетах Участников платежной системы переводы денежных средств не осуществляются.

6.2 Проверка достаточности денежных средств на Счетах Участников платежной системы определяется исходя из остатка денежных средств, находящихся на Счете Участника платежной системы на начало дня, и с учетом сумм денежных средств, списанных и зачисленных на Счет Участника платежной системы до определения достаточности денежных средств на Счете Участника платежной системы.

6.3 В случаях, предусмотренных законодательством или Договором банковского счета, достаточность денежных средств на Счетах Участников платежной системы определяется с учетом:

- сумм денежных средств, подлежащих списанию со Счета Участника платежной системы и (или) зачислению на Счет Участника платежной системы на основании распоряжений, принятых к исполнению и не исполненных до определения достаточности денежных средств на Счете Участника платежной системы;
- иных сумм денежных средств в соответствии с законодательством или Договором банковского счета.

6.4 В Платежной системе не предусмотрено создание гарантийного фонда.

7. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ МЕЖДУ ОПЕРАТОРОМ ПЛАТЕЖНОЙ СИСТЕМЫ И УЧАСТНИКАМИ ПЛАТЕЖНОЙ СИСТЕМЫ

7.1 Порядок взаимодействия с Участниками платежной системы

7.1.1 Взаимодействие Оператора платежной системы и Участника платежной системы при обмене неплатежной информацией, за исключением обмена информацией, предусмотренной разделом 16 Правил, осуществляется путем направления сообщений на электронную почту Оператора платежной системы (PS Sberbank@sberbank.ru), если Правилами и Договором банковского счета не предусмотрено иное.

7.1.2 Взаимодействие между Оператором платежной системы и Участниками платежной системы при проведении расчетов осуществляется с использованием распоряжений в электронном виде и (или) на бумажном носителе в соответствии с системой доставки, определенной Договором банковского счета с Участником платежной системы.

7.1.3 Порядок взаимодействия Оператора платежной системы и Участника платежной системы устанавливается заключаемыми между ними Договором банковского счета и Договором присоединения, предусматривающими принятие Участником платежной системы условий настоящих Правил в целом

без каких-либо изъятий и оговорок.

7.2 Порядок предоставления Участниками платежной системы информации о своей деятельности Оператору платежной системы:

7.2.1 Для получения услуг по переводу денежных средств Участники платежной системы предоставляют Оператору платежной системы документы, предусмотренные Договором банковского счета.

7.2.2 Для осуществления контроля за соблюдением Правил платежной системы Участник платежной системы предоставляет Оператору платежной системы документы и информацию в порядке, предусмотренном разделом 17 настоящих Правил.

7.2.3 По запросу Оператора платежной системы Участники платежной системы предоставляют финансовую и иную информацию о своей деятельности Оператору платежной системы в течение 10 (десяти) календарных дней с момента получения запроса.

8. ПРАВА И ОБЯЗАННОСТИ УЧАСТНИКОВ

8.1 Участник обязан:

8.1.1 Своевременно и в полном объеме исполнять свои денежные обязательства перед Оператором платежной системы, плательщиками и получателями при осуществлении переводов денежных средств, включая оплату комиссий.

8.1.2 Обеспечивать наличие на своем Счете/Счетах у Оператора платежной системы остатков денежных средств, достаточных для осуществления расчетов.

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

8.1.4 Самостоятельно обеспечить техническую и технологическую возможность своего участия в Платежной системе в соответствии с требованиями настоящих Правил.

8.1.5 Для бесперебойного автоматического осуществления расчетов согласовать с Оператором платежной системы стандарты и принципы, используемые в программном обеспечении.

8.1.6 Извещать Оператора платежной системы о возможных рисках, связанных с изменениями программного обеспечения, применяемого при осуществлении расчетов.

8.1.7 Принимать меры по обеспечению конфиденциальности ключевой информации, используемой в средствах защиты.

8.1.8 Сохранять в тайне сведения по вопросам технологии электронного обмена, за исключением случаев, предусмотренных законодательством Российской Федерации.

8.1.9 Выполнять требования федеральных законов Российской Федерации, иных нормативных правовых актов, нормативных актов Банка России и Договора банковского счета при совершении операций и при оформлении распоряжений.

8.1.10 Соблюдать ограничения, предусмотренные Федеральным законом №161-ФЗ, при переводе электронных денежных средств.

8.1.11 В случае внесения изменений в документы, предоставленные при открытии Счета, а также при изменении других данных Участника, предоставить указанные изменения Оператору в срок, установленный Договором банковского счета.

8.1.12 Обеспечить контроль наличия, полноты и передачи в составе расчетных документов следующей информации о плательщике:

- о физическом лице, индивидуальном предпринимателе или физическом лице, занимающемся в установленном законодательством Российской Федерации порядке частной практикой: фамилии, имени, отчества (если иное не вытекает из закона или национального обычая), номера банковского счета, идентификационного номера налогоплательщика (при его наличии) либо адреса места жительства (регистрации) или места пребывания;
- о юридическом лице: наименования, номера банковского счета, идентификационного номера налогоплательщика или кода иностранной организации;
- обеспечить неизменность информации, содержащейся в полученном распоряжении, и ее хранение.

8.2 Участник имеет право:

8.2.1 Участвовать в других платежных системах.

8.2.2 Получать от Оператора платежной системы информацию по переводу денежных средств на основании письменного запроса.

8.2.3 Использовать наименование Платежной системы при размещении информационных/рекламных материалов Участника платежной системы в СМИ и иных источниках информации, при условии предварительного согласования с Оператором платежной системы.

8.2.4 Осуществлять иные действия, предусмотренные Договором банковского счета и настоящими Правилами.

9. ПРИМЕНЯЕМЫЕ ФОРМЫ БЕЗНАЛИЧНЫХ РАСЧЕТОВ

9.1 Основанием для осуществления безналичных расчетов при переводе денежных средств являются распоряжения Участников платежной системы, предусмотренные Положением Банка России от 29 июня 2021 г. № 762-П «О правилах осуществления перевода денежных средств».

9.2 Участник платежной системы от своего имени составляет распоряжение на перевод денежных средств в соответствии с заключенным с клиентом договором и действующим законодательством Российской Федерации.

9.3 Оператор платежной системы обязан информировать Участников платежной системы по их требованию об исполнении платежного поручения не позднее следующего рабочего дня после получения соответствующего обращения, если иной срок не предусмотрен Договором банковского счета.

9.4 Оператор платежной системы и Участники платежной системы не вмешиваются в договорные отношения между клиентами. Взаимные претензии по расчетам между ними, кроме возникших по вине Оператора платежной системы или Участников платежной системы,

решаются в установленном законодательством порядке без участия Оператора платежной системы и Участников платежной системы.

10. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЕРЕВОДА ДЕНЕЖНЫХ СРЕДСТВ В РАМКАХ ПЛАТЕЖНОЙ СИСТЕМЫ, ВКЛЮЧАЯ МОМЕНТЫ НАСТУПЛЕНИЯ ЕГО БЕЗОТЗЫВНОСТИ, БЕЗУСЛОВНОСТИ И ОКОНЧАТЕЛЬНОСТИ

10.1 При осуществлении переводов денежных средств в рамках Платежной системы Участник платежной системы использует формы безналичных расчетов, предусмотренные Положением Банка России от 29.06.2021 № 762-П «О правилах осуществления перевода денежных средств». Переводы денежных средств в иностранной валюте, в том числе, на территории Российской Федерации, осуществляются в соответствии с требованиями законодательства, регулирующего осуществление перевода денежных средств в иностранной валюте на территории Российской Федерации, с использованием форм и каналов связи, определенных Договором банковского счета.

10.2 Перевод денежных средств осуществляется за счет денежных средств Участника платежной системы, находящихся на его Счете.

10.3 Перевод денежных средств осуществляется в рамках применяемых форм безналичных расчетов посредством зачисления денежных средств на Счет.

10.4 Безотзывность, безусловность, окончательность перевода денежных средств в рамках Платежной системы при направлении денежных средств одним из Участников ПС другому Участнику ПС через Оператора платежной системы в соответствии с Федеральным законом №161-ФЗ наступают:

а) безотзывность - при отсутствии или прекращении возможности отзыва распоряжения об осуществлении перевода денежных средств со Счета Участника-плательщика в определенный момент времени;

б) безусловность - при отсутствии условий или выполнении Участником (или его клиентом) всех условий для осуществления перевода денежных средств в определенный момент времени;

в) окончательность - при предоставлении денежных средств получателю средств в определенный момент времени. В момент наступления окончательности перевода денежных средств обязательство по переводу денежных средств Оператора платежной системы перед Участником(ами) прекращается.

11. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖНОГО КЛИРИНГА И РАСЧЕТА

11.1 Взаимодействие между Оператором платежной системы и Участниками платежной системы при предоставлении Участникам платежной системы операционных услуг, услуг платежного клиринга и расчетных услуг осуществляется с использованием распоряжений в электронном виде и (или) на бумажном носителе в соответствии с Договорами банковского счета, заключаемыми между Оператором платежной системы и Участником платежной системы.

11.2 При платежном клиринге в платежной системе осуществляются:

11.2.1 выполнение процедур приема к исполнению распоряжений Участников платежной системы, в том числе, проверка соответствия распоряжений Участников платежной системы требованиям законодательства, определение достаточности денежных средств для исполнения распоряжений и определение платежных клиринговых позиций;

11.2.2 передача принятых распоряжений Участников платежной системы для исполнения в расчетный центр;

11.2.3 направление Участникам платежной системы извещений (подтверждений), касающихся приема к исполнению и исполнения распоряжений Участников платежной системы.

11.3 Определение платежной клиринговой позиции Участника платежной системы осуществляется платежным клиринговым центром Оператора на валовой основе в размере суммы индивидуального распоряжения Участника платежной системы, по которому Участник платежной системы является плательщиком или получателем средств.

11.4 После определения платежной клиринговой позиции на валовой основе распоряжения Участников платежной системы передаются Расчетному центру для исполнения.

11.5 Расчет в Платежной системе осуществляется Расчетным центром Оператора платежной системы посредством списания и зачисления денежных средств по Счетам Участников платежной системы на основании поступивших от платежного клирингового центра распоряжений в размере сумм платежных клиринговых позиций. В случае заключения между операторами платежных систем договора о взаимодействии платежных систем, предусмотренного п.п.3.4-3.5 Правил, Участником платежной системы может являться расчетный центр другой платежной системы, действующий по поручению оператора такой платежной системы.

11.6 Платежный клиринг и расчет осуществляются Оператором платежной системы в период времени, в течение которого выполняются процедуры приема к исполнению, отзыва, возврата (аннулирования) и исполнения распоряжений. Регламент функционирования Платежной системы установлен разделом 13 Правил и Приложением 3.

11.7 Удостоверение права распоряжения денежными средствами при приеме к исполнению распоряжения в электронном виде, контроль целостности распоряжения в электронном виде, а также проверка подлинности и контроль целостности заявления, запроса, ответа, уведомления, извещения в электронном виде при обмене электронными сообщениями с Участниками платежной системы осуществляются посредством проверки кода аутентификации (электронной подписи) Участника платежной системы, являющегося отправителем электронного сообщения.

11.8 Процедуры удостоверения права распоряжения денежными средствами, контроля целостности, структурного контроля и контроля значений реквизитов распоряжений на бумажном носителе выполняются в момент приема распоряжения путем проверки идентичности подписей и оттиска печати на распоряжении заявленным образцам и при вводе распоряжения в Платежную систему.

11.9 Контроль достаточности денежных средств при выполнении процедур приема к исполнению распоряжений проводится на валовой основе в пределах суммы денежных средств, определяемой суммой денежных средств, имеющихся на счете Участника платежной системы к моменту проведения контроля достаточности денежных средств с учетом суммы ограничений на распоряжение денежными средствами, распоряжение которыми ограничено в соответствии с законодательством Российской Федерации (арест и другие ограничения).

11.10 Контроль достаточности денежных средств на счете Участника платежной системы проводится по каждому распоряжению Участника платежной системы индивидуально по мере поступления распоряжений Участника платежной системы в течение операционного дня с учетом ранее поступивших и неисполненных распоряжений Участника платежной системы.

11.11 Контроль достаточности денежных средств завершается с положительным результатом,

если платежная клиринговая позиция Участника платежной системы не превышает сумму денежных средств, определяемую в соответствии с пунктом 11.9 настоящих Правил.

11.12 Если сумма денежных средств, распоряжение которыми должно быть ограничено в соответствии с законодательством Российской Федерации (арест и другие ограничения), превышает сумму денежных средств, находящихся на Счете Участника платежной системы, исполнение распоряжений не осуществляется до накопления на счете Участника платежной системы суммы, не меньшей, чем сумма денежных средств, распоряжение которыми должно быть ограничено.

11.13 После определения платежной клиринговой позиции распоряжения Участников платежной системы, для исполнения которых достаточно денежных средств, исполняются.

11.14 Распоряжения о переводе денежных средств со счетов Участников платежной системы, контроль достаточности денежных средств по которым не был положительным, откладываются и помещаются во внутридневную очередь распоряжений для проведения контроля достаточности денежных средств до окончания текущего операционного дня.

11.15 Распоряжения, не исполненные в течение текущего операционного дня по причине недостаточности денежных средств на счете Участника платежной системы, после окончания данного операционного дня и осуществления контроля достаточности денежных средств на банковском счете не принимаются к исполнению и возвращаются отправителям распоряжений не позднее рабочего дня, следующего за днем поступления распоряжения либо за днем получения акцепта плательщика, за исключением распоряжений отправителей и взыскателей средств, порядок исполнения которых установлен федеральным законодательством и/или Договором банковского счета.

11.16 При отрицательных результатах выполнения процедур приема к исполнению распоряжений распоряжения, подлежащие возврату (аннулированию), поступившие в электронном виде, аннулируются, а поступившие на бумажном носителе возвращаются составителю, при этом одновременно составителю направляется уведомление об отрицательных результатах выполнения процедур приема к исполнению распоряжений.

11.17 Участники платежной системы могут отзывать распоряжения и повторно направлять их. Распоряжение может быть отозвано Участником платежной системы путем направления по каналам связи, предусмотренным Договором банковского счета для передачи распоряжений на перевод денежных средств, запроса в электронном виде, содержащего реквизиты, позволяющие идентифицировать отзываемое распоряжение, представленное в электронном виде, для отзыва распоряжения, представленного на бумажном носителе.

11.18 Неисполненные распоряжения возвращаются Оператором платежной системы Участнику платежной системы в случаях их отзыва до наступления безотзывности перевода денежных средств. Отзыв распоряжений не осуществляется при наступлении безотзывности перевода денежных средств.

11.19 Перевод денежных средств осуществляется в соответствии с указанными в распоряжении Участника платежной системы номерами счетов плательщика, получателя средств, банка плательщика, банка получателя средств, а также БИК (SWIFT код) банка плательщика, БИК (SWIFT код) банка получателя средств.

11.20 Исполнение распоряжения подтверждается Оператором платежной системы путем направления Участнику извещения и/или выписки.

12. ОКАЗАНИЕ УСЛУГ ПЛАТЕЖНОЙ ИНФРАСТРУКТУРЫ

12.1 Общие положения:

12.1.1 Оператор платежной системы совмещает свою деятельность с деятельностью Расчетного центра, Платежного клирингового центра, Операционного центра (при совместном упоминании - Операторы услуг платежной инфраструктуры) в рамках одной организации, одновременно оказывая операционные услуги, услуги платежного клиринга и расчетные услуги.

12.1.2 Оператор платежной системы не привлекает Операторов услуг платежной инфраструктуры.

12.1.3 При оказании услуг платежной инфраструктуры Оператор платежной системы не вправе в одностороннем порядке приостанавливать (прекращать) оказание услуг платежной инфраструктуры Участникам платежной системы и их клиентам.

12.1.4 Оператор платежной системы в рамках предоставления услуг платежной инфраструктуры:

- имеет лицензию Банка России и иные правоустанавливающие документы на проведение операций (учредительные документы, сертификаты и т.п.), согласно действующему законодательству Российской Федерации;

- имеет размер уставного капитала не ниже, установленного законодательством Российской Федерации;

- гарантирует банковскую тайну в соответствии с законодательством Российской Федерации о банках и банковской деятельности;

- несет обязанность не раскрывать третьим лицам сведения об операциях и о Счетах Участников платежных систем и их клиентов, полученные при оказании операционных услуг, за исключением передачи информации в рамках Платежной системы, а также случаев, предусмотренных законодательством;

- обеспечивает защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, в соответствии с требованиями к защите указанной информации, установленными Правительством Российской Федерации;

- обеспечивает защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными Банком России, по согласованию с ФСБ и ФСТЭК;

- определяет регламент взаимодействия подразделений, осуществляющих функции Операционного центра, Платежного клирингового центра, Расчетного центра;

- обеспечивает процедуры технического взаимодействия информационных систем.

12.2 Требования к выполнению Оператором платежной системы функций Операционного центра.

12.2.1 Выполняя функции Операционного центра, Оператор платежной системы:

- обеспечивает для Участников платежной системы и их клиентов обмен электронными сообщениями между Участниками платежной системы, между подразделениями Оператора платежной системы (получение электронных сообщений, содержащих распоряжения участников платежной системы, передача указанных сообщений для осуществления клиринговых и расчетных операций);

- обеспечивает доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа;
- осуществляет передачу извещений (подтверждений) о приеме и об исполнении распоряжений Участников платежной системы;
- может осуществлять в соответствии с Правилами иные действия, связанные с использованием информационно-коммуникационных технологий и необходимые для функционирования Платежной системы;
- несет ответственность за реальный ущерб, причиненный Участникам платежной системы, вследствие неоказания (ненадлежащего оказания) операционных услуг.

12.2.2 Ответственность Оператора платежной системы за реальный ущерб при выполнении функций Операционного центра ограничивается размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) операционных услуг.

12.3 Требования к выполнению Оператором платежной системы функций Платежного клирингового центра.

12.3.1 Выполнение Оператором платежной системы функций Платежного клирингового центра осуществляется в соответствии с Правилами.

12.3.2 Платежный клиринговый центр Оператора платежной системы:

- передает от имени Участников платежной системы подлежащие исполнению распоряжения Участников платежной системы в Расчетный центр;

- несет ответственность за ущерб, причиненный Участникам платежной системы вследствие неоказания (ненадлежащего оказания) услуг платежного клиринга.

12.3.3 Ответственность Оператора платежной системы за ущерб при оказании услуг платежного клиринга ограничивается размером неустойки, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежного клиринга.

12.4 Требования к выполнению Оператором платежной системы функций Расчетного центра.

12.4.1 Оператор платежной системы осуществляет функции Расчетного центра в соответствии с Правилами и на основании Договоров банковского счета, заключаемых с Участниками платежной системы.

12.4.2 В рамках выполнения функций Расчетного центра Оператор платежной системы исполняет поступившие от подразделения, выполняющего функции Платежного клирингового центра, распоряжения Участников платежной системы посредством списания и зачисления денежных средств по Счетам Участников платежной системы в размере сумм определенных платежных клиринговых позиций.

12.4.3 Оператор платежной системы вправе выступать оператором УПИ и оказывать расчетные услуги другим платежным системам в качестве Расчетного центра в соответствии с Федеральным законом №161-ФЗ.

12.5 Информация о предоставлении услуг платежной инфраструктуры размещается на сайте Оператора платежной системы.

12.6 В случае приостановления или прекращения оказания услуг платежной инфраструктуры Оператор платежной системы уведомляет об этом Банк России и Участников в порядке и сроки, определенные п. 3.3 Правил.

12.7 Порядок оплаты услуг по переводу денежных средств и за оказание услуг платежной инфраструктуры:

12.7.1 Плата за услуги по переводу денежных средств взимается в соответствии с тарифами, установленными Оператором платежной системы, путем списания соответствующих сумм денежных средств со Счета Участника платежной системы. Действующие в рамках Платежной системы тарифы приведены в Приложении 4 к настоящим Правилам. Тарифы публикуются на официальном сайте Оператора платежной системы. При внесении изменений в Правила платежной системы, касающихся введения новых тарифов или увеличения размера тарифов, новые или увеличенные тарифы вводятся в действие не ранее чем через 30 календарных дней после дня уведомления Банка России и направления в его адрес изменений в Правила платежной системы с предоставлением расчетов, обосновывающих указанные изменения тарифов.

12.7.2 В случае недостаточности денежных средств на Счете для оплаты услуг Оператора платежной системы Оператор платежной системы не предоставляет Участнику платежной системы услугу по переводу денежных средств.

12.7.3 Установление минимального размера оплаты услуг по переводу денежных средств Участниками платежной системы и их клиентами запрещается.

12.7.4 Оператор платежной системы не взимает плату за оказание услуг платежной инфраструктуры.

13. ВРЕМЕННОЙ РЕГЛАМЕНТ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ

13.1 Платежная система функционирует ежедневно, включая выходные и нерабочие праздничные дни, установленные законодательством Российской Федерации. Перевод денежных средств Участников Платежной системы осуществляется в течение 1 (одного) дня, если иные сроки не предусмотрены Договором банковского счета.

13.2 Дата и время совершения любых действий Оператором платежной системы и Участниками платежной системы определяются по местному времени региона, в котором обслуживается счет Участника платежной системы.

13.3 Операционное время для исполнения распоряжений Участников платежной системы устанавливается в соответствии с Приложением 3.

13.4 Участники платежной системы извещаются об изменениях операционного времени Платежной системы в соответствии с условиями Договора банковского счета путем направления Участникам платежной системы информационных сообщений в электронном виде, а также размещения информации на официальном сайте Оператора платежной системы.

14. ОБЕСПЕЧЕНИЕ И ПОКАЗАТЕЛИ БЕСПЕРЕБОЙНОСТИ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ (БФПС)

14.1 В целях обеспечения бесперебойности функционирования Платежной системы (БФПС) Оператор платежной системы, Участники платежной системы обязаны предупреждать нарушения требований законодательства Российской Федерации, Правил платежной системы, заключенных договоров взаимодействия, а также восстанавливать функционирование Платежной системы в случае его нарушения.

14.2 Бесперебойным считается такое функционирование Платежной системы, когда Оператор платежной системы без приостановления (прекращения) функционирования на срок, превышающий установленный Правилами платежной системы, оказывает Участникам Платежной системы услуги платежной инфраструктуры (операционные и расчетные услуги и услуги платежного клиринга).

14.3 Приостановлением (прекращением) функционирования Платежной системы считается неоказание услуг платежной инфраструктуры и (или) неосуществление переводов денежных средств в рамках Платежной системы в течение 2 (двух) и более часов.

14.4 В случае нарушения БФПС Оператор платежной системы гарантирует восстановление функционирования:

- в течение 24-х часов - на уровне, необходимом для осуществления переводов денежных средств;

- в течение 72-х часов - на уровне, обеспечивающем оказание УПИ в соответствии с Регламентом функционирования Платежной системы, установленным разделом 13 Правил.

14.5 Правилами Платежной системы не устанавливаются:

- норматив времени для обмена электронными сообщениями. Ответ о доставке электронного сообщения формируется в системе, через которую производится обмен электронными сообщениями в соответствии с Договором банковского счета;

- норматив времени, предусмотренный для выполнения регламентных работ. Проведение профилактических работ, связанных с обновлением программного обеспечения, проводится за пределами времени функционирования Платежной системы.

14.6 Показатели БФПС, к которым относятся продолжительность восстановления оказания УПИ (П1), показатель непрерывности оказания УПИ (П2), показатель соблюдения регламента (П3), показатель доступности операционного центра ПС (П4), показатель изменения частоты инцидентов (П5), и их динамика определяют уровень/изменение уровня риска нарушения БФПС. Оператором платежной системы в целях анализа качества и бесперебойности функционирования Платежной системы рассчитываются указанные показатели БФПС согласно Приложению 2.

14.7 Поддержание показателей БФПС не ниже установленных минимально допустимых значений осуществляется в порядке, установленном настоящими Правилами.

14.8 Оператор платежной системы проводит оценку влияния на БФПС каждого произошедшего в платежной системе инцидента в срок не позднее окончания 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). Оценка влияния инцидента(ов) на БФПС осуществляется в порядке и по форме, приведенным в Приложении 2 Правил.

14.9 Ответственность Участников платежной системы за неисполнение порядка обеспечения БФПС определяется в соответствии с разделом 18 Правил.

15. УПРАВЛЕНИЕ РИСКАМИ В ПЛАТЕЖНОЙ СИСТЕМЕ

15.1 Под системой управления рисками в Платежной системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для бесперебойности функционирования платежной системы с учётом размера причиняемого ущерба.

15.2 Основной целью системы управления рисками в Платежной системе является обеспечение ее эффективного, надежного и бесперебойного функционирования.

15.3 Оператор платежной системы организует систему управления рисками, разрабатывая комплекс организационных и технических мероприятий в целях снижения вероятности возникновения неблагоприятных факторов и их последствий для БФПС, минимизации собственных потерь и потерь Участников платежной системы в случае реализации рисков.

15.4 Оператор платежной системы в лице Управляющего комитета по управлению рисками в Платежной системе проводит оценку системы управления рисками в Платежной системе и документально оформляет результаты указанной оценки.

15.5 Оператор платежной системы проводит плановую оценку рисков, а также внеплановые оценки рисков на основании методик анализа рисков в Платежной системе, анализа результатов применения способов управления рисками и с учетом составленных профилей рисков.

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

15.7 Внеплановая оценка рисков в платежной системе проводится Оператором платежной системы в отношении всех рисков в платежной системе при внесении изменений в один или несколько бизнес-процессов, в рамках которых обеспечивается оказание УПИ. Срок проведения внеплановой оценки не должен превышать:

- шести месяцев со дня внесения указанных изменений,
- четырех месяцев со дня возникновения/выявления событий, предусмотренных п.п.15.8.1-15.8.3 Правил.

15.8 Условия, вызывающие необходимость проведения внеплановой оценки отдельных рисков (отдельного риска), определены Регламентом управления рисками в Платежной системе «Сбербанк» № 4909-4 от 26.09.2023 г. (далее – Регламент №4909), при этом в целях соблюдения сроков внеплановой оценки особому контролю подлежат, в том числе:

15.8.1 события, реализация которых привела к приостановлению (прекращению) оказания УПИ и описание которых в профиле риска не предусмотрено, либо негативные последствия от их реализации превышают негативные последствия, предусмотренные для этих событий в профиле риска;

15.8.2 факты 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 платежной системы готов принять без применения способов управления рисками;

15.8.3 при выявлении существенного риска в платежной системе, для которого

уровень присущего риска до применения способов управления рисками в платежной системе может превысить или превысил уровень допустимого риска.

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

15.10 Критерии отнесения событий, реализовавшихся при оказании УПИ, к событиям приостановления оказания УПИ определены Оператором платежной системы в Регламенте №4909. К критериям приостановления оказания УПИ не относится приостановление оказания УПИ в связи с проведением технологических и (или) регламентных работ в случае, если Оператор заранее уведомил об этом участников платежной системы. Критерии пересматриваются не реже 1 раза в три года.

15.11 Система управления рисками Оператора ПС предусматривает реализацию следующих мероприятий, установленных ст. 28 Федерального закона №161-ФЗ.

Определение организационной структуры управления рисками, обеспечивающей контроль за выполнением Участниками платежной системы требований к управлению рисками

15.12 Модель управления рисками в Платежной системе предусматривает самостоятельное управление рисками Оператором платежной системы.

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

15.14 Система управления рисками предусматривает следующие способы управления рисками:

- осуществление расчета в пределах предоставленных Участниками платежной системы денежных средств;
- управление очередностью исполнения распоряжений Участников платежной системы;
- другие способы управления рисками, при необходимости дополнительно разрабатываемые Оператором платежной системы и учитывающие особенности функционирования Платежной системы и взаимодействия с Участниками платежной системы.

15.15 Органом по управлению рисками в Платежной системе является Управляющий комитет ПАО Сбербанк по управлению рисками в Платежной системе «Сбербанк» (далее - УК по управлению рисками в Платежной системе). При принятии решений обеспечивается учет интересов как Оператора платежной системы, так и Участников платежной системы.

15.16 В состав УК по управлению рисками в Платежной системе входят Председатель комитета, заместитель Председателя комитета, члены комитета - представители Оператора платежной системы, а также представители Участников платежной системы, ответственные за управление рисками. В состав УК по управлению рисками в Платежной системе могут быть включены представители Банка России с правом совещательного голоса.

15.17 Функции по управлению рисками в Платежной системе осуществляются следующими структурными подразделениями и сотрудниками Оператора платежной системы в соответствии с их полномочиями:

- подразделениями, оказывающими расчетные, операционные услуги и услуги платежного клиринга;
- структурными подразделениями / сотрудниками Оператора платежной системы, отвечающими, в том числе, за информационно-техническую поддержку и обеспечение защиты информации у Оператора платежной системы;
- иными подразделениями и сотрудниками в рамках их должностных обязанностей.

Определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений

15.18 Функции УК по управлению рисками в Платежной системе:

- утверждение внутренних нормативных документов по направлению деятельности УК по управлению рисками в Платежной системе;
- утверждение критериев оценки системы управления рисками;
- рассмотрение отчетов о рисках в Платежной системе;
- рассмотрение результатов оценки эффективности системы управления рисками в Платежной системе;
- проведение оценки системы управления рисками в Платежной системе, в том числе используемых методов оценки рисков в Платежной системе, результатов применения способов управления рисками в Платежной системе;
- формирование предложений и рекомендаций по итогам проведения оценки системы управления рисками в Платежной системе;
- выполнение прочих функций по организации и совершенствованию системы управления рисками в Платежной системе.

15.19 Подразделения, осуществляющие управление рисками в Платежной системе, выполняют следующие функции:

- идентификация, анализ и оценка рисков;
- мониторинг уровня риска в Платежной системе, разработка и проведение мероприятий, связанных с управлением рисками в Платежной системе;
- сбор, обработка и систематизация информации по управлению рисками, в том числе, в виде подготовки отчетов;
- своевременное информирование руководства Оператора платежной системы и/или Участника платежной системы об уровне риска;

• разработка плана(ов) обеспечения непрерывности деятельности и восстановления деятельности Оператора платежной системы при прекращении (приостановлении) оказания услуг платежной инфраструктуры;

• прочие функции в рамках управления рисками в Платежной системе.

15.20 Участники платежной системы самостоятельно определяют собственную организационную структуру управления рисками в соответствии с нормативными актами Банка России или законодательством, применимым к Участнику.

Доведение до органов управления Оператора платежной системы соответствующей информации о рисках

15.21 Отчет по результатам анализа рисков предоставляется УК по управлению рисками в Платежной системе не реже 2 раз в год, а также, при необходимости, доводится до Участников платежной системы.

15.22 Оценка (оценка эффективности) системы управления рисками в Платежной системе проводится УК по управлению рисками в Платежной системе не реже 1 (одного) раза в 3 (три) года в порядке, установленном распорядительными документами УК по управлению рисками в Платежной системе.

Определение показателей бесперебойности функционирования Платежной системы в соответствии с требованиями нормативных актов Банка России

15.23 Определение бесперебойного функционирования Платежной системы и показателей БФПС приведено в разделе 14 настоящих Правил.

15.24 Оператор платежной системы осуществляет сбор и обработку сведений, используемых для расчета показателей БФПС, указанных в Приложении 2 настоящих Правил (далее - сведения по Платежной системе), а также сведений об инцидентах, предусмотренных внутренними нормативными документами Оператора. При привлечении поставщиков (провайдеров), предоставляющих услуги в сфере информационных технологий в целях оказания оператором УПИ услуг платежной инфраструктуры и (или) предоставляющих услуги обмена информацией при осуществлении операций, Оператор платежной системы оценивает риски, возникающие в связи привлечением сторонних поставщиков УПИ, и обеспечивает сбор от привлеченных операторов УПИ и обработку сведений, используемых для расчета показателей БФПС.

15.25 Оператор платежной системы анализирует показатели БФПС и использует результаты указанного анализа при оценке системы управления рисками в Платежной системе. Показатели БФПС могут пересматриваться по результатам анализа с периодичностью, установленной внутренними документами Оператора. Оператор платежной системы вправе вводить дополнительные показатели БФПС, в частности, при привлечении сторонних операторов УПИ.

15.26 Оператор платежной системы обеспечивает хранение сведений по Платежной системе и сведений об инцидентах в течение не менее пяти лет с даты получения указанных сведений. Сведения хранятся в электронном виде на сетевом ресурсе уполномоченного подразделения Оператора.

Определение порядка обеспечения бесперебойности функционирования Платежной системы

15.27 По результатам анализа рисков Оператор платежной системы оценивает потери от рисковых событий и разрабатывает план(ы) по обеспечению непрерывности и (или) восстановлению деятельности (ОНиВД) с учетом всех возможных сценариев развития событий, создающих угрозу БФПС.

15.28 .Оператор платежной системы разрабатывает и включает в план ОНиВД мероприятия, направленные на управление непрерывностью функционирования Платежной системы в случае возникновения инцидентов, связанных с приостановлением оказания УПИ или нарушением установленных уровней оказания УПИ, в том числе, мероприятия по переходу на резервный комплекс программных и (или) технических средств, а также мероприятия, осуществляемые в случае неработоспособности систем и сервисов, приводящих к приостановлению оказания УПИ.

15.29 В плане(ах) обеспечения непрерывности (восстановления) деятельности:

- определяется перечень угроз, нарушивших/способных нарушить бесперебойное функционирование Платежной системы или ее Участников, степень их воздействия на БФПС в зависимости от оценочной суммы ущерба/потерь (низкая, средняя, высокая);
- определяется перечень затронутых операционных процессов, в первую очередь, критически важных;
- устанавливается время и порядок действий для восстановления функционирования Платежной системы и ее компонент;
- определяются резервные компоненты функционирования Платежной системы (сетевые, вычислительные, электроснабжения и т.п.);
- приводится перечень мероприятий, предотвращающих возникновение рисковых событий (резервное копирование данных Платежной системы; перераспределение обязанностей, полномочий и процедур между подразделениями, сотрудниками, использование резервных мощностей, объектов, использование альтернативных процедур и способов исполнения распоряжений о переводе денежных средств и др.);
- определяется порядок информирования Участником Оператора платежной системы о нарушении функционирования.

15.30 Мероприятия и способы достижения и поддержания уровня рисков нарушения БФПС, предусмотренные планами по обеспечению непрерывности и (или) восстановлению деятельности, пересматриваются с периодичностью не реже 1 раза в год.

15.31 Обеспечение непрерывности и (или) восстановление функционирования осуществляется Оператором платежной системы в комплексе с другими мерами, направленными на минимизацию соответствующих рисков.

15.32 Оператор платежной системы проводит выбор и осуществляет реализацию мероприятий и способов достижения и поддержания уровня рисков нарушения БФПС, оценивает их эффективность и принимает меры по их совершенствованию. Стабильный уровень рисков нарушения БФПС в течение не менее 1 (одного) года свидетельствует об эффективности выбранных способов достижения и поддержания уровня рисков нарушения БФПС. В случае снижения уровня рисков Оператор платежной системы пересматривает используемые способы поддержания уровня рисков нарушения БФПС.

15.33 Оператор платежной системы анализирует факторы риска нарушения БФПС, способные оказать влияние на нарушение БФПС. Факторы риска нарушения БФПС могут носить внутренний (сбои функционирования АС, повреждение каналов связи) и внешний (правовой, техногенный и т.п.) характер.

15.34 Вероятность возникновения возможного нарушения определяется в зависимости от результатов оценки периодичности реализации рисковых событий.

Определение методик анализа рисков в Платежной системе, включая профили рисков

15.35 Существенными рисками в Платежной системе являются:

- операционный риск,
- правовой риск,
- риск кибербезопасности,
- риск ликвидности,
- риск нарушения БФПС.

15.36 Операционный риск - риск оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию услуг, вследствие возникновения у субъектов Платежной системы сбоев, отказов и аварий в работе информационных и технологических систем, недостатков в организации и выполнении технологических и управленческих процессов, ошибок или противоправных действий персонала субъектов Платежной системы либо вследствие воздействия событий, причины возникновения которых не связаны с деятельностью субъектов Платежной системы, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц.

15.37 Правовой риск - риск возникновения финансовых потерь (убытков) в результате:

- нарушения Банком и (или) Участниками ПС условий заключенных договоров;
- нарушения Банком и (или) Участниками ПС нормативных правовых актов;
- допускаемых правовых ошибок при осуществлении деятельности (например, неправильные юридические консультации или неверное составление документов, в том числе при рассмотрении спорных вопросов в суде);
- несовершенства правовой системы (противоречивость законодательства, отсутствие правовых норм по регулированию отдельных вопросов, возникающих в процессе деятельности Банка);
- нахождения филиалов Банка под юрисдикцией различных государств.

15.38 Риск кибербезопасности (риск информационной безопасности) - риск реализации угроз безопасности информации, которые обусловлены недостатками процессов обеспечения информационной безопасности, в том числе проведения технологических и других мероприятий, недостатками прикладного программного обеспечения автоматизированных систем и приложений, а также несоответствием указанных процессов деятельности со стороны Оператора и Участников платежной системы[2].

15.39 Риск ликвидности - риск невыполнения требования осуществить расчеты по обязательствам в полном объеме в срок исполнения платежа.

15.40 Риск нарушения БФПС - риск нарушения бесперебойности функционирования Платежной системы в результате превышения допустимого уровня одного или совокупности существенных рисков, при одновременном приостановлении (прекращении) функционирования ПС в течение 2 (двух) и более часов. Профиль риска нарушения БФПС представляет собой сводный профиль в отношении всех существенных рисков в платежной системе.

15.41 Основными этапами процесса управления рисками в Платежной системе являются:

- идентификация риска - выявление риска, определение причин и предпосылок его

[2] Соответствует риску информационной безопасности согласно Положению Банка России №716-П "О требованиях к системе управления операционным риском в кредитной организации и банковской группе" (далее - Положение №716-П) и Положению Банка России №719-П "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств" (далее - Положение №719-П).

возникновения;

- сбор и регистрация информации о событиях риска, в том числе, определение потерь и возмещений потерь;
- количественная и качественная оценка риска - анализ информации,
- полученной в результате идентификации риска, определение вероятности наступления негативных для Платежной системы последствий, разработка ключевых индикаторов риска, порядка их расчета и пороговых значений[3];
- выбор и применение способов реагирования на риск - разработка и проведение мероприятий по устранению причин, ограничению, снижению, предупреждению повышения риска и его последствий;
- контроль и мониторинг уровня риска - анализ риска в динамике его развития.

15.42 Оператор определяет профили существенных рисков, включая описание каждого риска, вероятность наступления риска, последствия реализации риска и прочие факторы.

15.43 Актуализация профилей рисков проводится по результатам плановой или внеплановой оценки всех рисков, а также внеплановой оценки отдельных рисков (отдельного риска) в Платежной системе. По результатам разработки/пересмотра профилей рисков определяются меры, реализуемые в рамках системы управления рисками.

15.44 Выявление и анализ рисков в Платежной системе, описание профилей рисков, определение уровня риска, характеризуемого вероятностью наступления рискового события и величиной возможных последствий, оценка системы управления рисками производятся Оператором платежной системы на основании методики анализа рисков, установленной Регламентом №4909.

15.45 В рамках оценки рисков Оператором платежной системы определяется вероятность наступления событий (действий), которые могут привести к возникновению потерь, возможные сценарии реализации рисков, оцениваются вероятность и последствия реализации рисков, размер потенциальных потерь, уровни рисков, выявляются изменения уровней рисков и профилей рисков.

15.46 Оценка системы управления рисками в Платежной системе осуществляется Оператором платежной системы на основе отчетов по рискам Платежной системы, заключения по результатам аудита системы управления рисками в Платежной системе и другой информации.

15.47 Оператор платежной системы проводит мониторинг и анализ рисков на постоянной основе.

15.48 Оператор платежной системы обеспечивает хранение сведений, содержащихся в профилях рисков, не менее пяти лет со дня составления и пересмотра (актуализации) профилей рисков.

Определение порядка обмена информацией, необходимой для управления

[3] В соответствии с Положением Банка России от 08.04.2020 № 716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группе» в качестве КИР операторов платежной системы рассматриваются показатели бесперебойности функционирования платежной системы (БФПС), установленные Положением Банка России от 03.10.2017 № 607-П "О требованиях к порядку обеспечения бесперебойности функционирования платежной системы, показателям бесперебойности функционирования платежной системы и методикам анализа рисков в платежной системе, включая профили рисков".

рисками

15.49 Оператор платежной системы определяет порядок взаимодействия с Участниками, направленный на достижение и поддержание уровня риска в Платежной системе. Порядок взаимодействия определяется Правилами и Договором банковского счета.

15.50 Оператор платежной системы в целях контроля за соблюдением обеспечения БФПС, управлением рисками и за соблюдением Правил платежной системы может направлять запросы Участникам платежной системы о предоставлении информации, необходимой Оператору платежной системы для осуществления вышеуказанного контроля, в том числе, осуществлении мониторинга и фиксирования информации, связанной с рисками в деятельности соответствующего Участника платежной системы, и их результатах, о доступном остатке денежных средств на счетах Участников платежной системы, возможных изменениях режимов функционирования и другие сведения.

Определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев

15.51 Ответственность Оператора платежной системы за неоказание (ненадлежащее оказание) услуг платежной инфраструктуры определяется в размере прямого действительного ущерба, причиненного Участнику(ам) платежной системы.

15.52 Оператор платежной системы должен информировать о случаях и причинах приостановления (прекращения) оказания УПИ Банк России и Участников платежной системы в порядке, установленном требованиями законодательства о платежной системе.

15.53 Оператор платежной системы проверяет соблюдение Участниками платежной системы бесперебойности функционирования путем сбора и анализа инцидентов, произошедших на стороне Участника и повлиявших на бесперебойность расчетов Участника и Оператора ПС.

15.54 Оператор платежной системы информирует Участника о выявленных нарушениях, при необходимости совместно с ним согласовывает мероприятия и сроки по устранению нарушений, осуществляет проверку результатов устранения нарушений. Результаты проверки направляются Участнику(ам) платежной системы, в деятельности которого(ых) выявлены нарушения.

Определение порядка изменения операционных и технологических средств и процедур

15.55 В случае принятия решения о модернизации или замене используемых операционных и технологических средств и процедур Оператор платежной системы:

- разрабатывает технические требования на создание и внедрение новых операционных и технологических средств и процедур;
- выбирает разработчика новых операционных и технологических средств и процедур;
- заключает договор с разработчиком;
- по завершении разработки производит тестирование новых операционных и технологических средств и процедур;
- осуществляет внедрение новых операционных и технологических средств и процедур.

Определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией

15.56 Оператор платежной системы определяет порядок изменения операционных и

технологических средств и процедур в рамках внутренних документов по управлению технологическими изменениями, касающимися предоставления УПИ и поддержки технологий по оказанию расчетных услуг. По решению Оператора платежной системы в порядке и в сроки, установленные условиями конкурсного отбора, для осуществления контроля и оценки качества и надежности операционных и технологических средств, информационных систем Платежной системы привлекается независимая организация, имеющая лицензию, необходимый опыт, навыки, а также, при необходимости, средства и оборудование, позволяющие осуществлять соответствующую оценку.

Порядок обеспечения защиты информации в Платежной системе

15.57 Описание порядка обеспечения защиты информации в Платежной системе приведено в разделе 16 настоящих Правил.

16. ТРЕБОВАНИЯ К ЗАЩИТЕ ИНФОРМАЦИИ

16.1 Участники и Оператор платежной системы обеспечивают защиту информации в соответствии с требованиями нормативно-правовых актов, включая требования Федерального закона "О национальной платежной системе" от 27.06.2011 № 161-ФЗ, Федерального закона "О персональных данных" от 27.07.2006 № 152-ФЗ, Постановления Правительства РФ от 13.06.2012 № 584 "Об утверждении Положения о защите информации в платежной системе", Положения Банка России от 04.06.2020 № 719-П "О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств" (далее - Положение № 719-П), Положения Банка России от 17.04.2019 № 683-П "Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента" (далее - Положение №683-П).

16.2 В Платежной системе функции по оценке и управлению рисками кибербезопасности распределяются между Оператором платежной системы и Участниками платежной системы.

16.3 Оператор осуществляет управление риском кибербезопасности в платежной системе как одним из видов операционного риска в порядке, установленном разделом 15 Правил, с учетом особенностей, определенных настоящим разделом. Оператор ПС, совмещая функции расчетного, операционного и платежного клирингового центра, обеспечивает выполнение требований Положения №719-П при оказании всех услуг платежной инфраструктуры.

16.4 Оператор платежной системы определяет требования к Участникам платежной системы в части системы управления рисками кибербезопасности.

16.5 Оператор и Участники обеспечивают защиту платежных документов на всех этапах жизненного цикла.

16.6 Оператор ПС обеспечивает[4]:

- требуемый уровень защиты информации для объектов информационной инфраструктуры, используемых для проведения расчетов;
- тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры не реже 1 (одного) раза в год;
- проведение оценки соответствия[5] уровням защиты информации с привлечением сторонних организаций, имеющих лицензию на осуществление деятельности по

[4] В соответствии с Положениями №№ 719-П, № 683-П, ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2-2018.
[5] В соответствии с Положением №719-П.

технической защите конфиденциальной информации, не реже 1 (одного) раза в 2 (два) года и хранение отчета, подготовленного проверяющей организацией, не менее 5 (пяти) лет с даты его выдачи;

- регистрацию результатов совершения собственных и клиентских действий, связанных с осуществлением доступа к защищаемой информации.

16.7 Технологические меры по обеспечению защиты информации при осуществлении переводов денежных денежный средств, включая меры по обеспечению защиты информации при осуществлении переводов денежных средств на технологических участках, в которые входят:

- идентификация, аутентификация и авторизация клиентов операторов по переводу денежных средств при совершении действий в целях осуществления переводов денежных средств;

- формирование (подготовка), передача и прием электронных сообщений; удостоверение права клиентов операторов по переводу денежных средств распоряжаться денежными средствами; осуществление переводов денежных средств;

- учет результатов осуществления переводов денежных средств; хранение электронных сообщений и информации об исполненных переводах денежных средств,

осуществляются Оператором в соответствии с требованиями Положения № 719-П и внутренними нормативными документами Оператора.

16.8 Оператор и Участники платежной системы самостоятельно управляют рисками кибербезопасности. Система управления рисками каждого Участника платежной системы должна включать, в том числе, назначение ответственных сотрудников и (или) наделение соответствующими полномочиями подразделений, ответственных за управление рисками и разработку внутренних правил по управлению рисками. Участники платежной системы несут ответственность за реализацию рисков кибербезопасности в их деятельности в соответствии с Правилами, требованиями законодательства Российской Федерации или законодательства, применимого к Участнику.

16.9 Оператор и Участники платежной системы принимают организационные и технические меры по обеспечению защиты информации в течение всего процесса обмена электронными сообщениями и другой информацией при осуществлении перевода денежных средств, в том числе:

- проводят мероприятия по анализу рисков и определению необходимых и достаточных мер защиты информации на основе этого анализа;
- создают и обеспечивают функционирование подразделения по защите информации или назначают работника, ответственного за организацию и осуществление защиты информации;
- обеспечивают контроль физического доступа к объектам информационной инфраструктуры;
- применяют, в том числе, некриптографические средства защиты информации от несанкционированного доступа, включая прошедшие в установленном порядке процедуру оценки соответствия.

16.10 Оператор и Участники платежной системы в соответствии с требованиями Банка России принимают меры антивирусной защиты своей информационной инфраструктуры, в числе которых обеспечивают:

- проведение регулярного (в случае технической возможности - в автоматическом режиме) обновления антивирусных баз и антивирусного ПО (далее - АВПО);
- проведение периодического сканирования АВПО системного и прикладного ПО;
- выполнение предварительной проверки АВПО устанавливаемого ПО;

- резервирование критичной информации;
- обучение сотрудников мерам антивирусной защиты.

16.11 В случае обнаружения вредоносного ПО (далее - ВПО), мероприятия Участника (Оператора платежной системы по минимизации ущерба от его воздействия на информационную инфраструктуру Участника) включают:

- определение источника заражения и путей дальнейшего распространения для организации действий по локализации заражения;
- удаление ВПО штатными средствами АВПО;
- обращение к разработчику АВПО для оказания технической поддержки в случае возникновения проблем при использовании штатного функционала АВПО;
- проверку целостности файлов прикладного и системного ПО, корректности работы ПО; - отправку Участником Оператору[6] платежной системы (Оператором Участнику[7]) уведомления[8] о зафиксированном факте воздействия ВПО в максимально короткий срок, но не позднее 24 часов с момента обнаружения данного факта.

16.12 В случае выхода из строя или нарушения штатного функционирования по причине воздействия ВПО АС/СВТ, задействованных в процессе осуществления переводов денежных средств, Участником / Оператором ПС может применяться приостановка переводов денежных средств на период устранения последствий воздействия ВПО.

16.13 Уведомление о факте воздействия ВПО направляется через контактных лиц, способы связи с которыми определяются в индивидуальном порядке (п.16.15 настоящего Порядка).

16.14 Участники платежной системы предоставляют Оператору платежной системы отчет об инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее - Отчет) ежемесячно (далее - отчетный период), не позднее пятого рабочего дня, следующего за месяцем, в котором были выявлены инциденты. Отчет должен содержать: даты возникновения и устранения инцидента, описание инцидента, меры, принятые для его устранения и предупреждения его возникновения в дальнейшем. В случае, если в течение отчетного периода инциденты в Платежной системе Участником выявлены не были, отправка Отчета не является обязательной для Участника.

16.15 Участник направляет на электронный адрес Оператора spss@sberbank.ru контакты как минимум одного своего должностного лица или подразделения, ответственного за взаимодействие с Оператором по вопросам выявления инцидентов, связанных с защитой информации в Платежной системе, а также по вопросам, связанным с управлением рисками кибербезопасности. Участник платежной системы обязан своевременно сообщать об изменении этих контактных данных. Оператор предоставляет Участникам аналогичные контактные данные и направляет информацию об их изменении. В случае необходимости передачи персональных данных обмен ими осуществляется в соответствии с требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных».

16.16 В случае выявления инцидента, для устранения которого необходимо привлечение Оператора платежной системы, Участник платежной системы не позднее следующего рабочего дня информирует Оператора платежной системы об этом инциденте и о том, что требуется его участие в устранении инцидента. Оператор информирует Участника аналогичным образом, в случае выявления им инцидента, для устранения которого требуется привлечение Участника.

16.17 Участники ПС и Оператор обязаны информировать Банк России:

- о выявленных инцидентах защиты информации;

[6] В зависимости от того, на чьей стороне зафиксирован инцидент.
[7] В зависимости от того, на чьей стороне зафиксирован инцидент.
[8] В случае масштабного воздействия вредоносного кода, по решению Оператора (Участника).

- о планируемых мероприятиях по раскрытию информации об инцидентах защиты информации[9], включая размещение информации на официальных сайтах в сети "Интернет", не позднее одного рабочего дня до дня проведения мероприятия.

16.18 Оператор платежной системы проводит работу по получению от Участников информации, необходимой для целей анализа обеспечения в платежной системе защиты информации при осуществлении переводов денежных средств, показателям уровня риска кибербезопасности, а также по оценке соответствия в отношении прикладного программного обеспечения автоматизированных систем и приложений Участников, включая применение Участниками средств криптозащиты, посредством анкетирования в сроки и порядке, установленные в соответствии с п.п.17.5 - 17.8 настоящих Правил.

16.19 Оператор платежной определяет следующий порядок проведения работ по разработке, сертификации и (или) оценке соответствия в отношении прикладного программного обеспечения автоматизированных систем и приложений[10], задействованных на технологическом участке Платежной системы в инфраструктуре Участника (далее - Прикладное ПО):

16.19.1 для Участников, разрабатывающих Прикладное ПО самостоятельно:

- разработка должна осуществляться в соответствии с принципами SDLC[11] и лучшими мировыми практиками;
- Прикладное ПО должно сопровождаться технической и эксплуатационной документацией;
- Прикладное ПО, с учетом особенностей функционирования, должно содержать базовые механизмы безопасности, такие как:
  - администрирование и управление доступом;
  - идентификация и аутентификация;
  - контроль целостности;
  - контроль конфиденциальности;
  - контроль доступности;
  - криптографическая защита;
  - аудит;

Прикладное ПО подлежит обязательной сертификации в случаях, определяемых законодательством РФ.

Участник вправе провести оценку соответствия Прикладного ПО в соответствии с Федеральным законом от 27.12.2002 № 184-ФЗ «О техническом регулировании».

16.19.2 для всех Участников:

- введение Прикладного ПО в промышленную эксплуатацию допускается только после успешного прохождения приемо-сдаточных испытаний;
- введение Прикладного ПО в промышленную эксплуатацию производится на основании утвержденного организационно-распорядительного документа Участника.

16.20 Участники обеспечивают доступ своих работников только к той информации, которая необходима для выполнения должностных обязанностей. В должностные обязанности работников, участвующих в обработке информации, должны быть внесены требования по

[9] В соответствии с Положением №719-П.
[10] Включая ПО платежных приложений, предоставляемых Участникам внешними поставщиками платежных приложений.
[11] Security Data Life Cycle - безопасный жизненный цикл.

защите информации.

16.21 Участниками и Оператором используются технические средства защиты информации, в том числе:

- средства межсетевого экранирования, анализирующие проходящий через них сетевой трафик и имеющие возможность блокировки сетевых соединений, не попадающих под заранее установленные правила сетевого взаимодействия; на средствах межсетевого экранирования должно быть настроено правило, запрещающее прямой доступ из внешней сети к защищаемым ресурсам платежной инфраструктуры, а также ограничивающие доступ элементов платежной инфраструктуры к ресурсам сети Интернет, не связанным с выполнением переводов денежных средств;
- средства VPN или защищенного обмена информацией при использовании сети Интернет в качестве транспортной среды передачи данных;
- средства антивирусной защиты;
- средства обнаружения и предотвращения вторжений;
- средства анализа защищенности.

16.22 Для проведения работ по обеспечению защиты информации Участники и Оператор вправе привлекать организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации. При этом до начала работ со сторонней организацией -

исполнителем работ (оказанию услуг) по обеспечению защиты информации должно быть заключено Соглашение о неразглашении конфиденциальной информации. Договором на проведение работ (оказание услуг) по обеспечению защиты информации должна быть предусмотрена ответственность сторонней организации за оказание услуг по защите информации ненадлежащего качества, а также ответственность (в том числе финансовая) за инцидент информационной безопасности, произошедший в ходе выполнения работ, или вследствие оказания услуг по защите информации ненадлежащего качества, а также возмещение потерь (ущерба).

16.23 Оператор платежной системы обеспечивает учет и ведение информации о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

16.24 Оператор платежной системы информирует Участников о выявленных в платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств путем размещения данной информации на сайте Оператора платежной системы. Указанная информация обновляется ежегодно.

16.25 По запросу Участника платежной системы Оператор платежной системы вправе направить Участнику платежной системы информацию о методиках анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств.

16.26 Участники и Оператор реализуют мероприятия по противодействию осуществлению переводов денежных средств без согласия клиента в порядке, определенном Указанием Банка России от 08.10.2018 № 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу

денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента», а именно:

- выявляют операции, соответствующие признакам осуществления перевода денежных средств без согласия клиента;
- выявляют операции, совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры оператора по переводу денежных средств;
- выявляют случаи и осуществляют сбор технических данных по компьютерным атакам на объекты информационной инфраструктуры, которые могут привести к случаям и/или попыткам осуществления переводов денежных средств без согласия клиента;
- осуществляют сбор сведений об обращениях плательщиков в правоохранительные органы (при их наличии);
- принимают меры по выявлению и устранению причин и последствий компьютерных атак и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента;
- определяют в документах, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объема совершаемых клиентами оператора по переводу денежных средств операций в соответствии с частью 5.1 статьи 8 Федерального закона № 161-ФЗ;

и другие мероприятия, установленные Указанием № 4926-У.

16.27 Участники и Оператор обязаны реализовывать мероприятия по противодействию осуществлению переводов денежных средств без согласия клиента в порядке, установленном законодательством. Участники должны направлять в Банк России информацию обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента по форме и в порядке, установленными Банком России. Оператор и Участники обязаны обеспечивать значение формируемого на ежеквартальной основе показателя, характеризующего уровень переводов денежных средств без согласия клиента, не более 0,005 процента[12].

16.28 В целях реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента Оператор применяет систему выявления и мониторинга переводов денежных средств без согласия клиента в Платежной системе, функционирующую на основе следующих базовых принципов:

- интеграция с АС ФРОД-мониторинг[13];
- контроль целостности входящего потока переводов денежных средств в автоматическом режиме;
- выявление переводов с признаками необычности и/или подозрительности (необычные дата/время, сумма, локация, устройство), проверки по ряду других параметров;
- проверка переводов денежных средств на предмет выявления признаков мошеннических операций по базе данных АС ФРОД-мониторинг.

16.29 В целях противодействия осуществлению переводов денежных средств без согласия клиента Участник ПС обязан реализовать систему выявления и мониторинга переводов

[12] В соответствии с Положением №719-П.
[13] Система непрерывного наблюдения, выявления, регистрации, а также предотвращения событий, связанных с мошенническими схемами.

денежных средств без согласия клиента, позволяющую выявлять признаки осуществления переводов денежных средств без согласия клиента в соответствии с Приказом Банка России «Признаки осуществления перевода денежных средств без согласия клиента» от 27.09.2018 №ОД-2525. Участник ПС также обязан:

- анализировать качество внутренних правил и политик контроля на регулярной основе и своевременно вносить в них изменения;
- использовать свою систему обработки данных или ПО для контроля уровня неправомерных операций, составления отчетов и расследования подозрительной деятельности клиентов;
- проводить мероприятия по повышению уровня безопасности платежей и использовать соответствующие инструменты для снижения уровня переводов денежных средств без согласия клиента.

16.30 Участники в рамках своей системы управления рисками кибербезопасности обязаны:

- осуществлять управление риском кибербезопасности как одним из видов операционного риска;
- определить организационную структуру по управлению риском кибербезопасности;
- реализовать процессы выявления и идентификации риска кибербезопасности в отношении объектов информационной инфраструктуры;
- выявлять и анализировать риски кибербезопасности;
- установить состав показателей уровня риска кибербезопасности;
- контролировать уровень риска кибербезопасности.

16.31 Процессы выявления и идентификации рисков кибербезопасности Участников платежной системы должны быть направлены на идентификацию событий, действий, условий, которые могут оказать влияние на информационные системы и бизнес-процессы, реализующие услуги в рамках Платежной системы, а также определение возможных последствий, анализ причин и источников возникновения событий рисков кибербезопасности.

16.32 Выявление и идентификация риска кибербезопасности Участниками платежной системы должна включать следующие способы, но не ограничиваясь:

- анализ событий риска кибербезопасности;
- анализ динамики количественных показателей, направленных на измерение и контроль уровня риска кибербезопасности в определенный момент времени;
- интервью с работниками Участника платежной системы, в рамках которых работниками и руководством Участника обсуждаются риски кибербезопасности, оказывающие влияние на Платежную систему;
- анализ актов проверок, судебных актов (решений, определений, постановлений) и (или) актов исполнительных органов государственной власти, Банка России в части фактов, относящихся к реализации риска кибербезопасности;

- анализ информации уполномоченного подразделения и внешнего аудита;
- анализ информации работников Участника платежной системы, полученной в рамках инициативного информирования работниками Участника службы управления рисками и (или) службы внутреннего аудита;
- анализ других внешних и внутренних источников информации и способов выявления рисков кибербезопасности.

16.33 Участник платежной системы должен использовать результаты процедуры выявления и идентификации рисков кибербезопасности для проведения процедур количественной и (или) качественной оценки рисков кибербезопасности и корректного учета связи идентифицированного риска с событиями риска кибербезопасности. Участники платежной системы самостоятельно определяют методику оценки рисков кибербезопасности, включающую в себя порядок оценки воздействия и вероятности реализации риска кибербезопасности.

16.34 В рамках анализа и оценки рисков кибербезопасности Участники платежной системы должны выполнять следующие действия, но не ограничиваясь:

- проводить анализ и оценку внешних и внутренних факторов, влияющих на кибербезопасность информационных систем и бизнес-процессов, реализующих услуги в рамках Платежной системы;
- учитывать результаты идентификации угроз, нарушителей и уязвимостей кибербезопасности, существующие меры защиты информационных систем и бизнес-процессов, реализующих услуги в рамках Платежной системы;
- сопоставлять фактический уровень идентифицированного и оцененного риска кибербезопасности с установленным уровнем допустимого риска кибербезопасности и, при наличии, установленными ограничениями по риску кибербезопасности, применять способы управления риском кибербезопасности;
- вести мониторинг рисков кибербезопасности, в том числе контролировать их соответствие допустимым уровням риска и, при наличии, установленным ограничениям по риску, и, при необходимости, принимать решение о применении других способов управления рисками кибербезопасности в дополнение к ранее выбранным способам.

16.35 Участники платежной системы осуществляют контроль и мониторинг риска кибербезопасности в целях своевременного выявления ситуаций, требующих принятия мер реагирования. Мониторинг должен осуществляться в том числе путем отслеживания количественных и качественных показателей уровня риска кибербезопасности.

16.36 Участники платежной системы должны самостоятельно установить пороговые значения и осуществлять мониторинг количественных показателей уровня риска кибербезопасности, установленных Положением №716-П. Количественные показатели уровня риска кибербезопасности используются в целях оценки текущего уровня риска и подверженности риску путем соотнесения наблюдаемого уровня с пороговым значением. Участниками обеспечивается контроль за фактическими значениями контрольных показателей уровня риска кибербезопасности, а также реагирование в случае превышения пороговых (сигнальных и контрольных) значений. Пороговые значения показателей подлежат ежегодному пересмотру и актуализации.

16.37 Обязательными количественными показателями уровня риска кибербезопасности, подлежащими доведению до сведения Оператора, являются:

- общая сумма валовых прямых потерь и сумм величин косвенных потерь Участника в результате наступления событий риска кибербезопасности, связанных с осуществлением переводов денежных средств в Платежной системе, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года;

- отношение суммы валовых прямых потерь, понесенных организацией при выполнении функций Участника, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года, к общей сумме операций переводов денежных средств Участником в Платежной системе за этот же период;

- общая сумма валовых прямых потерь и косвенных потерь Участника в результате событий риска кибербезопасности у третьих лиц, привлеченных Участником для осуществления деятельности в Платежной системе, за отчетный период (первый квартал, полугодие, девять месяцев, год) нарастающим итогом с начала календарного года.

16.38 Для каждого показателя уровня риска кибербезопасности должны быть установлены:

- пороговые значения (сигнальное и контрольное), при превышении которых должны применяться меры, направленные на снижение уровня риска кибербезопасности, с обоснованием их установления;

- порядок реагирования в случае превышения пороговых значений, в том числе процедуры эскалации;

- периодичность расчета, порядок пересмотра и актуализации.

16.39 Участник платежной системы не осуществляет мониторинг не применимых к нему показателей уровня риска кибербезопасности, указанных в п.16.37 Правил. В этом случае Участник должен предоставить по запросу Оператора платежной системы обоснование исключения такого показателя уровня риска кибербезопасности.

16.40 Участник платежной системы может устанавливать дополнительные к приведенным в п.16.37 Правил показатели уровня риска кибербезопасности.

16.41 Сведения об установленных показателях уровня риска кибербезопасности, их пороговых и фактических значениях Участники платежной системы должны предоставлять Оператору по запросу. Порядок и сроки предоставления сведений устанавливаются Оператором

16.42 Участники платежной системы должны уведомлять Оператора платежной системы о факте(ах) нарушения ими установленных пороговых значений показателей уровня риска кибербезопасности через контактных лиц, способы связи с которыми определяются в индивидуальном порядке (п.16.15 Правил), не позднее следующего рабочего дня с момента выявления превышения.

16.43 В случае выявления факта(ов) превышения Участниками ПС «Сбербанк» пороговых значений показателей уровня риска кибербезопасности, оператор ПС вправе ввести ограничения параметров операций перевода Участниками ПС денежных средств. Решение об ограничениях осуществления Участником переводов денежных средств принимаются Управляющим комитетом ПАО Сбербанк по управлению рисками в Платежной системе «Сбербанк». В

качестве ограничений к Участнику могут быть применены, в частности, ограничения по сумме и/или количеству переводов денежных средств, приостановление проведения платежей на согласованный с Участником срок устранения выявленных нарушений. При получении от Участника информации о доведении значений показателей уровня риска кибербезопасности до установленных значений, либо о проведении мероприятий по устранению выявленных нарушений Оператор ПС принимает решение о достаточности/недостаточности проведенной Участником работы по снижению уровня риска кибербезопасности и о возможности снятия установленных ограничений на осуществление переводов денежных средств.

16.44 Участники и Оператор не вправе раскрывать третьим лицам сведения об операциях и о счетах Оператора или Участников, а также об операциях и счетах клиентов Оператора или Участников, за исключением передачи информации в рамках Платежной системы и случаев, предусмотренных федеральным законодательством.

16.45 Участники и Оператор обеспечивают регистрацию и хранение (в бумажном и/или электронном виде) в течение не менее 5 (пяти) лет[14] результатов контроля организационных мер по защите информации, а также контроля применения технических средств защиты информации. Порядок регистрации и хранения результатов контроля определяется Участниками и Оператором самостоятельно, с учетом того, что такой порядок должен обеспечить возможность проведения на основе результатов контроля своевременного разбора спорных или проблемных ситуаций.

16.46 Оператор самостоятельно определяет требования и порядок защиты информации при осуществлении переводов денежных средств в Правилах и в своих внутренних нормативных документах, и вправе вносить в них изменения при пересмотре порядка обеспечения защиты информации в случаях:

- выявления уязвимостей и недостатков в Платежной системе по результатам контрольных мероприятий или оценки соответствия;
- изменения требований законодательства Российской Федерации, в том числе требований Банка России к обеспечению защиты информации в национальной платежной системе.

16.47 Участники, присоединяясь к Правилам, исполняют требования Оператора, предъявляемые к защите информации и системе управления рисками кибербезопасности в Платежной системе, а также обеспечивают выполнение требований к защите информации и системе управления рисками кибербезопасности, предъявляемых законодательством РФ, в том числе, требований Банка России.

16.48 Участники Платежной системы вправе предпринимать на свое усмотрение дополнительные меры по нейтрализации актуальных угроз безопасности информации, выявленных в ходе проведенных мероприятий по анализу рисков, и уведомлять о принятых мерах Оператора, в том числе направлять предложения о внесении изменений в Правила в части порядка обеспечения защиты информации при осуществлении переводов денежных средств.

16.49 Состав и порядок применения организационных мер защиты информации, не предусмотренных настоящими Правилами, определяется Оператором и Участниками самостоятельно, на основании результата мероприятий по анализу рисков.

16.50 В целях анализа мер по защите информации при осуществлении переводов денежных средств в Платежной системе Участники, по запросу Оператора, направляют ему, в том числе,

[14] В соответствии с Положением №719-П.

следующие сведения по обеспечению защиты информации, отражаемые в формах обязательной статистической отчетности Банка России, установленных Указанием от 14.06.2012 № 2831-У "Об отчетности по обеспечению защиты информации при осуществлении переводов денежных средств операторов платежных систем, операторов услуг платежной инфраструктуры, операторов по переводу денежных средств":

- о степени выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- о результатах проведенных оценок соответствия;
- о выявленных угрозах и уязвимостях в обеспечении защиты информации.

16.51 Информацию о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, Участники направляют в электронном виде контактному ответственному лицу либо подразделению Оператора в порядке и сроки, установленные п.16.16 настоящих Правил.

16.52 Участники, помимо выполнения требований настоящих Правил, в целях совершенствования системы защиты информации и управления рисками кибербезопасности вправе руководствоваться российскими и международными стандартами, а также лучшими мировыми практиками.

17. ПОРЯДОК ОСУЩЕСТВЛЕНИЯ КОНТРОЛЯ ЗА СОБЛЮДЕНИЕМ ПРАВИЛ

17.1 Оператор платежной системы осуществляет контроль за соблюдением Правил Участниками платежной системы, в том числе, за соблюдением требований законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, и в части, касающейся защиты информации.

17.2 В случае подтверждения факта несоблюдения Правил Участником платежной системы, Участник обязан устранить данное несоблюдение в срок, не превышающий 30 календарных дней, и направить информацию об его устранении Оператору платежной системы.

17.3 Оператор платежной системы осуществляет контроль за соблюдением Участниками платежной системы положений и требований Правил Платежной системы путем проведения проверок.

17.4 Для осуществления проверки Оператор платежной системы вправе:

- требовать у Участника платежной системы предоставления информации и документов (при необходимости) для проведения анализа на предмет соответствия требованиям Правил Платежной системы;
- получать устные и письменные разъяснения по вопросам деятельности Участника платежной системы в рамках Платежной системы.

17.5 Проверка Участника платежной системы осуществляется Оператором платежной системы путем направления Участнику платежной системы анкеты (опросного листа). Анкета содержит сведения, необходимые для предоставления Оператору платежной системы для проверки соблюдения требований настоящих Правил. Полный состав информации и формат анкеты (опросного листа) определяется Оператором платежной системы.

17.6 Участник платежной системы обязан предоставить полностью заполненную анкету и документы, предусмотренные анкетой, или мотивированный отказ от их предоставления, не

позднее 20 (двадцати) календарных дней с момента получения от Оператора платежной системы запроса о предоставлении анкеты, если иной срок не установлен запросом Оператора.

17.7 Обязательному контролю за соблюдением Правил подлежат Участники платежной системы, удовлетворяющие одному из следующих критериев:

- объем оборотов по операциям Участника, проводимым в рамках ПС, исчисляемый суммарно за 3 календарных месяца, предшествующих месяцу, в котором начинается проверка, превышает 10 млрд. в рублевом эквиваленте;
- нарушение Участником(ами) в течение 3 календарных месяцев, предшествующих месяцу, в котором начинается проверка, бесперебойности проведения расчетов по платежам клиентов более 5 рабочих дней подряд в связи с недостаточностью средств на Счете.

17.8 Период проверки по установленным критериям определяется Оператором и не зависит от срока давности присоединения Участника к Правилам. При этом выборочной проверке не подлежат участники, присоединившиеся к Платежной системе менее 6 календарных месяцев назад.

17.9 Данные критерии утверждаются и, при необходимости, пересматриваются УК по управлению рисками в Платежной системе.

17.10 Периодичность проведения проверки за соблюдением Участниками платежной системы Правил, удовлетворяющим критериям, определенным п.17.7, - не реже 1 (одного) раза в год. Периодичность проведения проверки за соблюдением всеми Участниками платежной системы Правил платежной системы - не реже 1 (одного) раза в 3 (три) года.

17.11 Оператор осуществляет анализ предоставленных Участниками анкет и готовит сводный отчет, включающий:

- оценку соблюдения Участниками требований к обеспечению защиты информации при осуществлении переводов денежных средств;
- оценку принимаемых Участниками мер по выявлению и предотвращению инцидентов операционного риска и по обеспечению непрерывности и восстановления деятельности (ОНиВД);
- выводы о влиянии/отсутствии влияния фактов несоблюдения Участниками Правил на бесперебойность функционирования Платежной системы и о соблюдении/несоблюдении Участниками Правил в целом.

17.12 В случаях повторного выявления фактов, свидетельствующих о несоблюдении Участниками Правил, Оператор доводит данную информацию до соответствующего Участника, запрашивает у него необходимые разъяснения и отчет о принятых мерах по устранению выявленных недостатков. Оператор вправе принять решение о сроках и порядке дополнительного анкетирования таких Участников.

18. ОТВЕТСТВЕННОСТЬ ЗА НЕСОБЛЮДЕНИЕ ПРАВИЛ

18.1 За неисполнение или ненадлежащее исполнение обязательств по настоящим Правилам, включая обязательства по обеспечению БФПС, Стороны несут ответственность в соответствии с действующим законодательством Российской Федерации и условиями Правил.

18.2 В случае нарушения одной из Сторон условий Правил, в результате которого другой Стороне были причинены убытки, виновная Сторона возмещает их в полном объеме.

18.3 Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение обязательств, если это неисполнение явилось следствием обстоятельств непреодолимой силы, возникших в результате событий чрезвычайного характера, которые Стороны не могли ни предвидеть, ни предотвратить разумными мерами (форс-мажор).

18.4 О наступлении и прекращении форс-мажорных обстоятельств, Сторона, не исполнившая обязательства в силу этих обстоятельств, обязана в течение 3 (трех) дней письменно уведомить Оператора платежной системы. Доказательством наличия и продолжительности форс-мажорных обстоятельств могут служить документы, выдаваемые компетентными органами Российской Федерации.

18.5 Возмещение убытков не освобождает виновную Сторону от надлежащего исполнения принятых обязательств и соблюдения настоящих Правил.

19. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ПРАВИЛА

19.1 Оператор вносит изменения и/или дополнения в Правила в порядке, предусмотренном настоящим разделом.

19.2 Оператор обеспечивает размещение проекта изменений в Правила платежной системы на сайте Оператора в срок не менее чем за 2 (два) месяца до утверждения изменений. Участники обязаны самостоятельно отслеживать информацию, размещаемую на сайте Оператора платежной системы. Оператор платежной системы оставляет за собой право информировать Участников о предполагаемых изменениях по другим каналам связи.

19.3 В случае возникновения предложений по предполагаемым изменениям Правил, Участники могут направить свое мнение Оператору платежной системы в срок не позднее 1 (одного) месяца со дня размещения информации на сайте Оператора платежной системы или получения информации от Оператора платежной системы по другому каналу связи.

19.4 Участнику, направившему в установленный пунктом 19.3 срок замечания об изменении Правил, Оператор платежной системы направляет разъяснение по обстоятельствам, требующим внесения изменений в Правила, либо размещает указанное разъяснение на сайте. Отсутствие заявления Участника о несогласии с изменениями Правил или полученными разъяснениями Оператора платежной системы по изменениям Правил по истечении 1 (одного) месяца со дня размещения информации на сайте и совершение Участником операций по Счету является подтверждением согласия Участника с изменениями Правил платежной системы. Изменения в Правила, получившие в установленный срок отрицательное мнение более половины всех Участников, подлежат доработке и повторному размещению на сайте Оператора платежной системы для ознакомления Участников.

19.5 Срок предварительного ознакомления Участников и внесения изменений в Правила, установленный п.19.2, может быть менее 2 (двух) месяцев при согласии всех Участников с вносимыми изменениями.

19.6 Оператор платежной системы представляет в Банк России изменения Правил платежной системы, изменения перечня операторов услуг платежной инфраструктуры (при необходимости) не позднее 10 (десяти) дней со дня утверждения (подписания) уполномоченным лицом (исполнительным органом).

19.7 Изменения в Правила, за исключением изменений, указанных в п. 12.7.1, вступают в силу со дня размещения на сайте Оператора платежной системы редакции Правил, получившей

отметку Банка России о соответствии требованиям законодательства о национальной платежной системе.

19.8 При изменении сведений об Операторе платежной системы, указанных при его регистрации, Оператор платежной системы уведомляет Банк России в течение 3 (трех) рабочих дней после дня наступления таких изменений.

20. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ В РАМКАХ ПЛАТЕЖНОЙ СИСТЕМЫ В НЕСТАНДАРТНЫХ И ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЯХ

20.1 Нестандартной ситуацией признается ситуация, не предусмотренная правилами обмена, установленными Договором банковского счета или сложившейся (стандартной) банковской практикой, на разрешение которой в рамках Платежной системы требуется более 60 минут.

20.2 Чрезвычайной ситуацией признается ситуация, повлекшая за собой нарушение регламентов взаимодействия между Оператором платежной системы и Участниками платежной системы более чем на 60 минут, к последствиям которого относятся:

- нарушение нормального функционирования основных автоматизированных систем, реализующих перевод денежных средств в Платежной системе;
- неработоспособность (недоступность) основных каналов связи, обеспечивающих передачу данных между Оператором платежной системы и Участниками платежной системы;
- отсутствие физической возможности нахождения работников Оператора платежной системы и Участников платежной системы на рабочих местах вследствие пожара, наводнения, аварий, актов террора, диверсий, саботажа, стихийных бедствий и других обстоятельств неодолимой силы;
- иные случаи, повлекшие нарушение нормального взаимодействия Оператора платежной системы и Участников платежной системы более чем на 60 минут.

20.3 В случае наступления нестандартной или чрезвычайной ситуации (далее при совместном упоминании - ЧС), оказывающей влияние на бесперебойность функционирования Платежной системы, а также в целях своевременного принятия мер, направленных на недопущение повышения риска неработоспособности Платежной системы, Участники платежной системы незамедлительно информируют Оператора платежной системы о возникших ЧС, о мерах, направленных на ликвидацию сбоев, вызванных ЧС, а также о возможных причинах и последствиях ЧС.

20.4 Информирование Оператора платежной системы осуществляется Участником платежной системы любым доступным способом: направлением факса, электронного письма в адрес подразделения Оператора платежной системы, задачи которого связаны с обеспечением непрерывности бизнеса, в исключительных случаях - посредством телефонной связи.

20.5 Информационное сообщение о возникших ЧС должно содержать следующую информацию:

- дату и время возникновения ЧС;
- характер ЧС;
- причины ЧС (в случае, если такие причины известны на момент подготовки сообщения);
- последствия ЧС;

- прогнозируемые сроки восстановления в случае, если в результате наступления ЧС было нарушено функционирование программно-технических средств, обеспечивающих деятельность по переводу денежных средств, и способы устранения нарушения функционирования программно-технических средств, обеспечивающих деятельность по переводу денежных средств.

20.6 По получению уведомления Оператор платежной системы, при необходимости, информирует Участников платежной системы о возникшей ситуации по электронной почте с последующим направлением уведомления в письменной форме.

20.7 Оператор платежной системы после получения информации о ЧС определяет действия Участника(ов) по каждой конкретной ЧС и осуществляет все возможные меры по урегулированию ситуации, а также недопущению критичных сбоев в работе Платежной системы, вплоть до отключения Участника(ов), допустившего(их) ЧС, от Платежной системы.

20.8 При прекращении обстоятельств, указанных в п.п. 20.1 и 20.2 настоящих Правил, Оператор Платежной системы оповещает Участника(ов) платежной системы об урегулировании (устранении) ЧС и отсутствии ее дальнейшего влияния на бесперебойность функционирования Платежной системы.

20.9 В случае возникновения обстоятельств непреодолимой силы, непредотвратимых при данных условиях, вызвавших операционные сбои и препятствующих осуществлению Сторонами своих функций по переводу денежных средств, и иных обстоятельств, не зависящих от воли Сторон, Стороны освобождаются от ответственности за неисполнение или ненадлежащее исполнение взятых на себя обязательств на время действия указанных обстоятельств.

21. ПОРЯДОК ДОСУДЕБНОГО РАЗРЕШЕНИЯ СПОРОВ С УЧАСТНИКАМИ ПЛАТЕЖНОЙ СИСТЕМЫ

21.1 В случае возникновения спорных ситуаций с клиентами Участник платежной системы самостоятельно и за собственный счет разрешает указанные ситуации, связанные с непрохождением перевода, отсутствием технологического обеспечения, а также иными причинами, вызванными действиями/бездействием Участника платежной системы или привлеченных им третьих лиц.

21.2 Споры, возникающие в процессе деятельности в рамках Платежной Системы, разрешаются в досудебном порядке путем рассмотрения претензий, направленных Участниками платежной системы в адрес Оператора платежной системы /Участника, в течение 20 (двадцати) рабочих дней с момента получения Оператором (Участником) письменной претензии Участника (Оператора).

21.3 Претензия должна содержать пояснение фактических обстоятельств и дату их возникновения, указание на то, с каким именно действием/бездействием Участника (Оператора) Оператор (Участник) не согласен, принятые к моменту направления претензии меры. Претензия может быть передана по любому из согласованных каналов связи: в электронной форме, подписанная квалифицированной электронной подписью, на бумажном носителе нарочным или по почте.

21.4 По результатам рассмотрения претензии Оператором платежной системы (Участником) составляется и направляется Участнику (Оператору платежной системы) письменный ответ о мерах, принятых в связи с поступившей претензией.

21.5 В целях урегулирования спорной ситуации, в связи с которой направлялась претензия, по инициативе Оператора платежной системы и/или Участника/Участников (далее - Стороны) может быть создана Согласительная комиссия, в которую войдет равное количество представителей Сторон.

21.6 Полномочия членов Согласительной комиссии подтверждаются доверенностями. Председатель Согласительной комиссии не избирается, члены Согласительной комиссии имеют равные права. Срок рассмотрения спорной ситуации Согласительной комиссией не может превышать 10 (десяти) рабочих дней.

21.7 Результаты работы Согласительной комиссии отражаются в Акте, который подписывается всеми членами комиссии. Члены комиссии, не согласные с выводами большинства, подписывают указанный Акт с возражениями, которые прилагаются к Акту. Акт составляется в таком количестве экземпляров, чтобы каждая из Сторон имела по одному подлинному экземпляру Акта.

21.8 В случае уклонения какой-либо из Сторон от участия в работе Согласительной комиссии, другая Сторона вправе самостоятельно провести заседание Согласительной комиссии с участием экспертов и составить соответствующий Акт.

21.9 Расходы, связанные с работой Согласительной комиссии, возлагаются на Сторону, инициировавшую проведение согласительной процедуры, если иное не будет определено Сторонами - участниками Согласительной комиссии.

21.10 Разногласия, не урегулированные в рамках досудебной процедуры, разрешаются в соответствии с законодательством Российской Федерации в Арбитражном суде г.Москвы.

21.11 Оператор платежной системы ведет реестр претензий и предложений Участников, содержащий реквизиты Участника, существо, дату и номер обращения, существо, дату и номер ответа, ответственного исполнителя Оператора платежной системы, отметку о повторном обращении со ссылкой на первичное обращение/претензию (при наличии). Претензии и предложения оперативно рассматриваются в сроки, не превышающие указанные в п.21.2.

Приложение 1

Договор присоединения № _____
к Платежной системе «Сбербанк»

г. “ ” _____ 202___ г.
(Место заключения)

Публичное акционерное общество «Сбербанк России», именуемое в дальнейшем “Оператор платежной системы”, в лице _____ действующего в соответствии с Уставом на основании

_____

_____

(наименование документа, подтверждающего полномочия)

с одной стороны, и

_____

(полное наименование кредитной организации)

именуемый в дальнейшем “Участник Платежной системы”, в лице

_____

(наименование должности, фамилия, имя и отчество уполномоченного лица)

с другой стороны, и совместно именуемые в дальнейшем “Стороны”, заключили настоящий Договор о нижеследующем:

1. ОСНОВНЫЕ ПОНЯТИЯ

1.1. Термины, используемые в настоящем Договоре, определены Правилами Платежной системы «Сбербанк» (далее - Правила), являющимися неотъемлемой частью настоящего Договора.
1.2. Правила ПС размещены на веб-сайте Оператора платежной системы http://www.sberbank.ru/ru/credit org/bankingservice/corespondent relations.

2. ПРЕДМЕТ ДОГОВОРА

2.1. Предметом настоящего Договора является присоединение Участника платежной системы в порядке ст. 428 Гражданского кодекса Российской Федерации и ч.7.ст.20 161-ФЗ «О национальной платежной системе» к участию в работе Платежной системы «Сбербанк» (далее - «Платежная система») на условиях Правил ПС.
2.2. Заключая настоящий Договор, Участник Платежной системы выражает согласие с Правилами ПС полностью.

3. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ СТОРОН

3.1. Права, обязанности и ответственность Сторон при работе в Платежной системе определяются Правилами ПС и настоящим Договором.

4. ДЕЙСТВИЕ ДОГОВОРА

4.1. Настоящий Договор вступает в силу с момента подписания обеими Сторонами.
4.2. Настоящий Договор может быть расторгнут в случаях, предусмотренных действующим законодательством Российской Федерации, Правилами ПС и настоящим Договором. Расторжение настоящего Договора не является основанием для закрытия Счета.
4.3. При расторжении Договора по инициативе Участника Платежной системы Участник Платежной системы направляет Оператору Платежной системы оригинал заявления о расторжении Договора на бумажном носителе, подписанного уполномоченным лицом и заверенного оттиском печати Участника Платежной системы.
4.4. Со дня поступления Оператору Платежной системы официального заявления Участника Платежной системы о расторжении настоящего Договора Оператор Платежной системы прекращает проведение операций по переводу денежных средств в рамках Платежной системы.
4.5. Расторжение настоящего Договора не влечет за собой прекращение обязательств Сторон по настоящему Договору, возникших до даты расторжения Договора и не освобождает Сторон от ответственности за выполнение обязательств, возникших при исполнении условий настоящего Договора.
4.6. Расторжение настоящего Договора не влечет за собой прекращение обязательств Сторон по Договору банковского счета.

5. ИНЫЕ УСЛОВИЯ

5.1. Участник Платежной системы, подписав настоящий Договор, подтверждает, что ознакомлен и согласен с тем, что Оператор Платежной системы вправе в одностороннем порядке вносить изменения в Правила ПС и Тарифы Платежной системы в порядке, установленном Правилами ПС.

Настоящий Договор составлен в 2 (двух) экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

6. МЕСТОНАХОЖДЕНИЕ И РЕКВИЗИТЫ СТОРОН

Оператор Платежной системы:
Местонахождение
Корреспондентский счёт, БИК
ИНН _____ **SWIFT-код** _____
Телефон

Internet **E-mail**

Участник Платежной системы:
Местонахождение
Почтовый адрес (для получения корреспонденции) _____
Корреспондентский счёт, БИК _____
ИНН **SWIFT-код**
Телефон

Internet **E-mail**

7. ПОДПИСИ СТОРОН

Оператор Платежной системы

М. П.

Участник Платежной системы

М. П.

Приложение 2

Для оценки бесперебойного функционирования Платежной системы и уровня бесперебойности оказания услуг Оператор платежной системы устанавливает следующие показатели БФПС, характеризующие качество функционирования операционных и технологических средств платежной инфраструктуры:

Показатели бесперебойности функционирования Платежной системы

	Показатели	Содержание	Мониторинг	Пороговый уровень показателя БФПС
1.	П1 - продолжительность восстановления оказания УПИ	Период времени восстановления оказания УПИ по каждому из инцидентов в случае приостановления оказания УПИ (ЧЧ.ММ.СС)	Постоянно (в разрезе УПИ)	<02:00:00
2.	П2 - показатель непрерывности оказания УПИ	Период времени между двумя последовательно произошедшими в ПС событиями, приведшими к нарушению оказания УПИ (ЧЧ.ММ.СС)	Постоянно (в разрезе УПИ)	> 24:00:00
3.	П3 - показатель соблюдения регламента	Степень соблюдения регламента, учитывающая отклонение от времени начала, времени окончания, продолжительности и последовательности процедур при оказании УПИ (%)	Постоянно (в разрезе УПИ)	> 98,00%
4.	П4 - показатель доступности ОЦ ПС	Фактическая продолжительность времени оказания операционных услуг за исключением продолжительности всех приостановлений оказания операционных услуг в %% к установленной продолжительности времени оказания операционных услуг (%)	Постоянно (по операционному центру)	> 98,00%

5.	П5 - показатель изменения частоты инцидентов	Темп прироста среднедневного количества инцидентов за календарный месяц по отношению к среднедневному количеству инцидентов за предыдущие 12 календарных месяцев, включая оцениваемый календарный месяц (%)	1 раз/месяц	0%

Пересмотр пороговых уровней показателей БФПС осуществляется не реже 1 (одного) раза в год с использованием результатов оценки рисков в Платежной системе.

Оператор ПС «Сбербанк» совмещает свою деятельность с деятельностью операторов УПИ в рамках одной организации, одновременно оказывая операционные услуги, услуги платежного клиринга и расчетные услуги. В этой связи пороговые показатели БФПС приведены и рассчитываются в целом по ПС, если иное не определено Правилами или нормативными документами.

Влияние инцидента(ов) на БФПС определяется Оператором платежной системы в соответствии с требованиями Положения №607-П:

	Последствия реализации инцидента	**Оценка влияния на БФПС**
1	По инциденту нарушен регламент выполнения процедур, но при этом не нарушен пороговый уровень показателей П1 и П2	Инцидент непосредственно не влияет на БФПС
2	По инцидентам, возникшим в течение календарного месяца, не нарушен пороговый уровень показателя П4, но одновременно нарушен пороговый уровень показателя П3 и (или) показателя П5[15]	Инциденты непосредственно не влияют на БФПС
3	По инциденту нарушен регламент выполнения процедур при одновременном нарушении порогового уровня показателя П2	Инцидент влияет на БФПС
4	По инциденту нарушен пороговый уровень показателя П1	Инцидент влияет на БФПС
5	По инциденту превышена продолжительность времени, в течение которого должно быть восстановлено оказание УПИ, соответствующее требованиям к оказанию услуг	Инцидент влияет на БФПС
6	По инцидентам, возникшим в течение календарного месяца, одновременно нарушены пороговые уровни показателей П3, П4, показателя П5	Инциденты влияют на БФПС

Повторная оценка произошедшего инцидента проводится в случае выявления дополнительных обстоятельств инцидента, оценка влияния которого на БФПС уже завершена.

[15] Здесь и далее - в части показателя П5 при оценке влияния инцидентов на БФПС учитывается отклонение фактического показателя П5 от нулевого значения

По всем инцидентам, произошедшим в Платежной системе в течение календарного месяца (строки 2, 6 таблицы), оценка влияния на БФПС проводится Оператором платежной системы в течение 5 (пяти) рабочих дней после дня окончания календарного месяца, в котором возникли инциденты.

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

К сведениям об инцидентах, используемых для расчета показателей БФПС, относятся:

- время и дата возникновения инцидента (в случае невозможности - время его выявления); краткое описание инцидента и его последствия;
- наименование бизнес-процесса(ов), в ходе которых произошел инцидент;
- наименование бизнес-процесса(ов), на которые инцидент оказал влияние;
- наличие (отсутствие) факта приостановления (прекращения) оказания УПИ в результате инцидента;
- влияние инцидента на БФПС;
- категория инцидента - степень влияния инцидента на функционирование ПС в зависимости от количества и значимости участников ПС, на которых оказал непосредственное влияние инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений участников ПС, и иных факторов (время и дата восстановления оказания УПИ в случае приостановления их оказания;
- время и дата восстановления оказания УПИ;
- мероприятия по устранению инцидента и его последствий с указанием планируемой и фактической продолжительности проведения данных мероприятий;
- дата восстановления оказания УПИ, соответствующего требованиям к оказанию услуг;
- неблагоприятные последствия инцидента, в том числе:
- сумма денежных средств, уплаченных Оператором платежной системы и (или) взысканных с Оператора платежной системы,
- количество и сумма неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников, на исполнение которых оказал влияние инцидент,
- продолжительность приостановления оказания УПИ.

Оператор платежной системы разрабатывает во внутренних документах регламенты выполнения взаимосвязанных последовательных технологических процедур (далее - регламенты выполнения процедур), устанавливающие время начала, время окончания, продолжительность и последовательность процедур, выполняемых при УПИ, в ходе которых может произойти инцидент.

Оператор платежной системы контролирует выполнение регламентов выполнения процедур по оказанию УПИ, а также определяет доступность операционных и технологических средств платежной инфраструктуры.

Приложение 3

РЕГЛАМЕНТ ФУНКЦИОНИРОВАНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ

Прием и исполнение распоряжений Участников

Операции	Местное время региона, в котором находится подразделение Оператора платежной системы, у которого открыт счет Участника)	
	рабочие дни*	выходные и праздничные дни
Прием распоряжений от Участников	02:00 до 21:30	В соответствии с Договором банковского счета
Исполнение распоряжений, направление подтверждений	02:00 - 22:00	Суббота: с 03:00 до 21 30 Воскресенье, праздничные дни: с 07:00 до 21 30
Направление выписки(ок) по Счетам	До 09:00 следующего рабочего дня*	До 09:00 следующего дня*

* если договором Счета не предусмотрено иное

Приложение 4

Тарифы за осуществление переводов денежных средств в рамках Платежной системы «Сбербанк»

№ п/п	Вид перевода	Тариф	
		в рублях	в иностранной валюте
1	**Зачисление** средств на Счет Участника платежной системы	бесплатно	бесплатно
2	**Списание денежных средств** со Счета Участника платежной системы, из них:		
	- с целью перевода средств на Счет другого Участника платежной системы, где плательщиком и/или получателем являются клиенты Участника Платежной системы	Max 12 руб.	Max 15 долл. США
	- с целью перевода средств на Счет другого Участника платежной системы, где плательщиком и получателем являются Участники платежной системы	Max 12 руб.	бесплатно
3	**Отзыв перевода**[16]	Max 200 руб.	45 долл. США

[16] Возврат средств по заявлению Участника платежной системы

Приложение 5

ПОРЯДОК
электронного документооборота
в Платежной системе «Сбербанк»

В целях настоящего приложения применяются термины и определения, установленные Правилами платежной системы «Сбербанк», а также:

Договор ДБО - договор предоставления услуг с использованием дистанционного банковского обслуживания Sber FinLine, заключаемый между Оператором платежной системы и Участником для подключения к СЭД.

Каналы связи - публичные сети связи, основанные на использовании протоколов TCP/IP, включая выделенные каналы связи и сеть Интернет.

Ключи шифрования - ключи, самостоятельно изготавливаемые представителями Участника с использованием программно-аппаратных средств Оператора платежной системы и предназначенные для обеспечения шифрования ЭД при их передаче через сеть Интернет.

Корректная ЭП - электронная подпись, дающая положительный результат ее проверки соответствующим сертифицированным средством ЭП, с использованием действующего на момент подписания ключа проверки ЭП его владельца.

Компрометация ключа ЭП - событие, определенное владельцем Сертификата как ознакомление неуполномоченным лицом (лицами) с его ключом ЭП (например, хищение, утеря носителя ключа ЭП, несанкционированное копирование или другие события, повлекшие за собой нарушение конфиденциальности ключа ЭП).

Программное обеспечение (ПО) - совокупность программ и программных документов, необходимых для их эксплуатации.

ПО «Клиентский модуль» - составная часть Системы, устанавливаемая на стороне Участника.

Система - система дистанционного банковского обслуживания Оператора платежной системы, предоставляющая Сторонам возможность осуществления электронного документооборота (приема/передачи документов с требуемым уровнем обеспечения информационной безопасности), а также позволяющая Участнику получать в режиме реального времени информацию о движении средств по Счету, статусах платежей и др.

Система электронного документооборота (СЭД) - совокупность ПО и технического оборудования, обеспечивающая процесс обмена электронными документами между Сторонами.

Стороны - стороны электронного документооборота по Договору ДБО - Оператор платежной системы и Участник.

Устройство «Электронный ключ» (Электронный ключ) - электронное устройство, обеспечивающее подключение к Системе и шифрование передаваемых данных, а также подписание отправляемых документов ЭП.

Электронный документ (ЭД) - электронный образ документа (платежного, служебно-информационного или иного), представленный в согласованном Сторонами формате, определяемом программными средствами создания документа.

Электронный платежный документ (ЭПД) - электронный документ (распоряжение Участника), являющийся основанием для совершения операций по Счету Участника. ЭПД, защищенные корректной ЭП, имеют равную юридическую силу с документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати Участника.

Электронный служебно-информационный документ (ЭСИД) - документ (запрос, выписка, подтверждение о проведении операции и т.п.), составленный одной Стороной и переданный другой Стороне в электронном виде, и обеспечивающий обмен информацией при совершении расчетов и проведении операций по Счету Участника. ЭСИД, защищенные корректной ЭП, в соответствии с законодательством РФ имеют равную юридическую силу с документами на бумажных носителях, подписанными собственноручными подписями уполномоченных лиц и заверенными оттиском печати Участника.

Термины «Электронная подпись» (ЭП), «Ключ электронной подписи», «Сертификат ключа проверки электронной подписи» (СКП ЭП), «Владелец сертификата ключа проверки электронной подписи» («Владелец сертификата») применяются в соответствии с Федеральным законом от 06.04.2011 №63-ФЗ «Об электронной подписи».

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий порядок электронного документооборота в Платежной системе «Сбербанк» устанавливает общие принципы осуществления электронного документооборота между Участниками (Сторонами).

1.2. Порядок не регулирует вопросы обмена электронными сообщениями, не являющимися ЭД.

1.3. Порядок применяется Сторонами с даты подписания договора присоединения при условии заключения Договора ДБО между Оператором платежной системы и Участником.

1.4. В рамках Платежной системы «Сбербанк», если иное не предусмотрено Договором банковского счета, при взаимодействии Сторон используются следующие каналы обмена ЭД с Оператором платежной системы:

- «Портал Sber FinLine», не требующий установки специализированного программного обеспечения на рабочее место Участника, работа Участника в Системе производится посредством браузера.
- «Шлюз ФИ (web-сервис) Sber FinLine», требующий установки ПО «Клиентский модуль» и заключения «Соглашения об обмене документами в электронном виде с кредитными организациями с использованием канала «Шлюз ФИ (web-сервис) Sber FinLine»». Взаимодействие Сторон при использовании шлюзовых решений осуществляется в порядке, установленном п.2.14 настоящего Приложения.
- Иная система доставки финансовых документов, использование которой согласовано Сторонами.

1.5. Участнику предоставляются следующие услуги по Счету с использованием Системы:

- прием от Участника и направление Участнику ЭПД, подписанных Корректной ЭП, на выполнение операций по Счету;
- предоставление Участнику в виде ЭСИД, подписанных Корректной ЭП, информации об операциях, совершенных по Счету, о статусах направленных Участником ЭПД и остатках средств по Счету Участника;
- прием от Участника и предоставление ему в виде ЭД, подписанных Корректной ЭП, информации свободного формата и т.д.

1.6. ЭД, подписанные Корректной ЭП, передаются и принимаются с использованием Системы и исполняются без их последующего предоставления на бумажных носителях.

2. УСЛОВИЯ ВЗАИМОДЕЙСТВИЯ

2.1. Программные и аппаратные средства Системы, средства защиты и средства связи эксплуатируются Сторонами за свой счет.

2.2. Подтверждение операций в Системе осуществляется Участником с использованием ЭП.

2.3. Электронные документы без ЭП не имеют юридической силы и в обработку Оператором платежной системы не принимаются.

2.4. Стороны признают все документы и информацию в электронном виде, направленные или полученные посредством Системы, содержащие Корректную ЭП, равнозначными документам на бумажном носителе, подписанным собственноручными подписями уполномоченных должностных лиц и заверенным печатями Сторон.

2.5. Участник получает услуги Системы через каналы связи и несет все риски, связанные с подключением его вычислительных средств к публичным каналам связи, возможным нарушением конфиденциальности и целостности информации при подключении к сети Интернет. Стороны также признают, что выход из строя рабочего места Системы, установленного у Участника, в результате вмешательства третьих лиц через сеть Интернет рассматривается как выход из строя по вине Участника.

2.6. При обмене ЭД между Сторонами, датой получения ЭД является дата доставки ЭД Системой, датой отправки - дата передачи документа в Систему.

2.7. Участник самостоятельно и за свой счет обеспечивает подключение своих вычислительных средств к сети Интернет, доступ к сети Интернет, а также обеспечивает защиту собственных вычислительных средств и ключей ЭП от несанкционированного доступа и вредоносного программного обеспечения.

2.8. Защиту информации при взаимодействии между программными средствами Участника и клиентской частью Системы, установленной у Участника, Участник обеспечивает самостоятельно и за свой счет.

2.9. Стороны признают в качестве единой шкалы времени при работе в Системе местное время по месту расположения подразделения Оператора платежной системы, оказывающего услуги по Договору банковского счета. Контрольным является время системных часов аппаратных средств подразделения Оператора платежной системы, оказывающего услуги по Договору банковского счета.

2.10. Оператор платежной системы исполняет поступившие от Участника ЭПД согласно условиям соответствующего Договора банковского счета.

2.11. Контроль за исполнением Оператором платежной системы ЭПД по Счету Участника осуществляется Участником самостоятельно путем просмотра в Системе состояния Счета и статусов документов.

2.12. Стороны признают, что:

- в соответствии с настоящим порядком Сторонами используется усиленная неквалифицированная электронная подпись в терминах Федерального закона от 06.04.2011 №63-ФЗ «Об электронной подписи»;
- после подписания ЭД ЭП любое изменение, добавление или удаление символов документа делает ЭП некорректной и проверка подписи по ключу проверки ЭП Участника дает отрицательный результат;
- создание Корректной ЭП ЭД возможно исключительно с использованием ключа ЭП;
- по содержанию ЭД, подписанных ЭП, и ключей проверки ЭП невозможно определить ключи ЭП;

- Участник несет полную ответственность за обеспечение конфиденциальности и сохранность своих ключей ЭП, а также за действия своего персонала;
- Участник может иметь несколько ключей ЭП, каждому ключу ЭП соответствует собственный ключ проверки ЭП;
- Участник самостоятельно формирует свои ключи ЭП;
- Заявление на сертификацию ключей ЭП на бумажном носителе, включающее реквизиты владельца ключа ЭП и содержание ключа проверки ЭП, заверенное собственноручной подписью уполномоченного лица, руководителя или другого должностного лица, наделенного соответствующими полномочиями, и оттиском печати Участника, предоставленное Оператору платежной системы, одновременно является документом, подтверждающим принадлежность Участнику данного ключа проверки ЭП;
- ЭД, подписанные Корректной ЭП Участника, а также системные журналы, ведущиеся в Системе, могут быть представлены Оператором платежной системы в качестве доказательств, в случае рассмотрения спора, возникшего в результате применения Системы;
- Участник самостоятельно формирует свои ключи шифрования, в том числе - для «Портала Sber FinLine». Запрос на выпуск сертификатов ключей шифрования формируется Участником с использованием средств Системы.

2.13. Порядок выпуска Сертификатов ключей проверки ЭП Участника определяется Договором ДБО.

2.14. В случае если Участником для взаимодействия выбран один из технологических вариантов поставки Системы: «Портал Sber FinLine» и/или «Шлюз ФИ (web-сервис) Sber FinLine»:

2.14.1 Взаимодействие между Сторонами в Системе осуществляется:

- через браузер, в случае выбора системы «Портал Sber FinLine»;
- посредством установки специализированного программного обеспечения на рабочем месте Участника в случае выбора канала доступа «Шлюз ФИ (web-сервис) Sber FinLine».

2.14.2 С Участником заключается Соглашение об обмене документами с кредитными организациями в электронном виде с использованием канала «Шлюз ФИ (web- сервис) Sber FinLine», определяющее порядок подключения и особенности обмена через канал «Шлюз ФИ (web-сервис) Sber FinLine».

2.14.3 Разграничение прав пользователей - уполномоченных лиц Участника в «Портале Sber FinLine» устанавливается на уровне Участника самостоятельно, исходя из собственных организационно-процессных ограничений. Участник может начать работу в «Портале Sber FinLine» с момента получения от Оператора платежной системы идентификатора Администратора в Системе и передачи Оператором платежной системы (посредством отправки электронного сообщения) Администраторам Участника на адреса электронной почты, указанные в заявлении на заключение договора Счета, уведомления, содержащего первоначальный пароль.

2.14.4 Обмен электронными документами между Сторонами через «Портал Sber FinLine» начинается с даты, указанной Участником в заявлении на заключение Договора ДБО либо в сообщении, направленном через «Портал Sber FinLine», но в любом случае - не ранее завершения выполнения всех необходимых для подготовки к осуществлению обмена процедур. Дата начала обмена электронными документами между Сторонами через Sber «Шлюз ФИ (web-сервис) Sber FinLine» определяется соответствующим Соглашением.

2.15. При компрометации или подозрении на компрометацию ключа ЭП Участника, в т.ч., при несанкционированном использовании или подозрении на несанкционированное использование Электронного ключа, Оператор платежной системы извещается о факте

компрометации ключа ЭП путем передачи соответствующего ЭД по Системе или иным доступным способом. Одновременно Участник прекращает передачу ЭД с использованием указанного Электронного ключа и выводит из действия соответствующие ключи ЭП. Оператор платежной системы, получивший сообщение о компрометации ключа ЭП, выводит соответствующий Сертификат ключа проверки ЭП из действия в максимально короткие сроки, но не позднее следующего рабочего дня после получения сообщения о компрометации. Скомпрометированные ключи ЭП для «Шлюз ФИ (web-сервис) Sber FinLine» уничтожаются Сторонами самостоятельно.

2.16. При утере/утрате Участником Электронного ключа Оператор платежной системы извещается о необходимости получения Участником нового устройства и о факте компрометации действующего Электронного ключа путем передачи соответствующего ЭД по Системе или иным доступным способом. Оператор платежной системы, получивший сообщение о компрометации Электронного ключа, блокирует в системе использование указанного Электронного ключа не позднее следующего рабочего дня после получения сообщения о компрометации.

2.17. Права и обязанности Оператора платежной системы и Участника при осуществлении электронного документооборота изложены в Договоре ДБО.

2.18. При возникновении разногласий и споров в связи с обменом ЭД с ЭП с помощью Системы с целью установления фактических обстоятельств, послуживших основанием для их возникновения, а также для проверки целостности и подтверждения авторства ЭД, Стороны обязаны провести техническую экспертизу. Процедура проведения технической экспертизы определена в Договоре ДБО и Соглашении об обмене документами с кредитными организациями в электронном виде с использованием канала «Шлюз ФИ (web-сервис) Sber FinLine».

2.19. Споры, по которым не достигнуто соглашение Сторон после проведения технической экспертизы, разрешаются в Арбитражном суде г. Москвы в соответствии с действующим законодательством Российской Федерации.