# Правила платежной системы UnionPay

(редакция №7 – Операционный бюллетень от «29» ноября 2019 года)

УТВЕРЖДАЮ:

Генеральный директор

ООО «ЮнионПэй»

_____ / г-н Фань Цзигуан

29 ноября 2019 г.

# Оглавление

# О документе

Настоящие правила платежной системы UnionPay в России в редакции №6 учитывают изменения, внесенные операционными бюллетенями от 27.10.2014, 30.10.2015, 11.12.2015, 17.08.2017, 19.10.2018, 17.12.2018. Настоящие правила платежной системы UnionPay в России в редакции №6 вступают в силу 03.03.2019 г. в соответствии с операционным бюллетенем от 17.12.2018.

**Цель**

Настоящие правила платежной системы UnionPay в России (далее – «**Правила**») установлены ООО «ЮнионПэй», выступающим в качестве оператора платежной системы UnionPay в России, на единых глобальных принципах использования банковских карт UnionPay с соблюдением требований законодательства РФ и распространяются на операции, осуществляемые на территории России.

**Ссылки на другие документы**

В Правилах могут содержаться ссылки на другие документы UnionPay по отдельным вопросам. Информация в этих документах, как правило, носит технический или операционный характер, и они применяются в том случае, если Участник участвует в оказании соответствующих услуг. В случае любых расхождений или противоречий между Правилами и другими документами UnionPay относительно операций по Картам UnionPay на территории России, преимущественную силу имеют положения Правил.

**Время и Место**

Если прямо не предусмотрено иное, ссылки на время в настоящем документе являются ссылками на московское время. Правила публикуются в сети Интернет на сайте www.unionpayintl.com/ru/ в разделе «*Правила UnionPay в России*».

**Термины и определения**

Термины, определенные в Федеральном законе от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» (далее – «**Закон о НПС**»), применяются в Правилах с уточнениями, указанными в настоящем разделе «**Термины и определения**» ниже.

**Банк России**

Центральный банк РФ (Банк России).

**БФПС**

Бесперебойность функционирования Платежной системы, (то есть способность предупреждать нарушения требований законодательства РФ, Правил, заключенных договоров при взаимодействии Субъектов платежной системы, а также восстанавливать надлежащее функционирование Платежной системы в случае его нарушения в течение времени, определенного в Правилах).

**Внутринациональная операция**

Операция, осуществленная на территории РФ посредством международных платежных карт (платежных карт, эмитированных кредитными организациями, расположенными в двух и более государствах, и на которых размещен единый товарный знак (знак обслуживания), принадлежащий иностранному юридическому лицу, личным законом которого считается право иностранного государства), и не являющаяся трансграничной операцией, как указано в Законе о НПС.

**Держатель карты**

Правомочный пользователь Карты UnionPay.

**Инцидент**

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

**Исходящие файлы**

Распоряжения Платёжного клирингового центра, направляемые им в Расчётный центр, содержащие реестр нетто-позиций.

**Карта UnionPay**

Любая банковская карта с логотипом «UnionPay» и банковским идентификационным номером, присвоенным или одобренным UnionPay, выданная на основе операционных и технических стандартов UnionPay. Данное определение также включает в себя любое электронное устройство платежа, которое держатель платежной банковской карты может использовать для осуществления операций по ней.

**Косвенный участник**

Участник платежной системы, соответствующий критериям, предъявляемым к Косвенным участникам, перечисленным в пункте 2.1.1 (*Критерии участия*) и пункте 2.1.2 (*Категории участников*) Правил, которому Прямой участник, являющийся оператором по переводу денежных средств, открывает банковский счет на основании соответствующего договора банковского счета в целях осуществления расчета с другими Участниками Платежной системы.

**Кредитный риск**

Риск оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию таких услуг, Расчетным центром вследствие невыполнения Участниками договорных обязательств перед указанной организацией в установленный срок или в будущем.

**Непокрытая позиция**

Дебетовая Платежная клиринговая позиция, для исполнения которой недостаточно денежных средств на Расчетном счете.

**НСПК**

Акционерное общество «Национальная система платежных карт».

**Общий коммерческий риск**

Риск оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию таких услуг, вследствие ухудшения финансового состояния Оператора платежной системы и (или) Операторов услуг платежной инфраструктуры, не связанного с реализацией Кредитного риска и Риска ликвидности.

**Оператор платежной системы**

ООО «ЮнионПэй» в качестве оператора Платежной системы UnionPay.

**Оператор услуг платежной инфраструктуры**

Операционный центр, Платежный клиринговый центр и Расчетный центр.

**Операция**

Серия взаимосвязанных сообщений, обрабатываемых в соответствии с Правилами. В зависимости от контекста, приобретение товаров или услуг, перевод денежных средств, снятие наличных в банкоматах, иные варианты перевода денежных средств, смена ПИН-кода в банкомате или запрос баланса.

**Операционный риск**

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

**Операционный центр**

Юридическое лицо, предоставляющее операционные услуги в соответствии с Законом о НПС.

**Партнер**

Организации (в том числе, банки), не присоединившиеся к Правилам, и заключившие партнерские соглашения (договоры) с Прямыми участниками, являющиеся клиентами Прямых участников для целей осуществления переводов денежных средств и последующих расчетов по операциям с использованием Карт UnionPay на территории Российской Федерации без участия Оператора платежной системы в качестве стороны по такому договору (партнерскому соглашению).

**Перевод с Карты на Карту**

Операция с использованием Карты UnionPay, результатом которой является перевод денежных средств отправителем (как Держателем карты, так и держателем карты иной платежной системы,) – плательщиком денежных средств (далее – «**Отправитель»**), Держателю карты – получателю (далее – «**Получатель**») на банковский счет Получателя либо увеличения остатка электронных денежных средств Получателя, совершаемая на основании распоряжения Отправителя.

**Платежная система**

Платежная система UnionPay, оператором которой является ООО «ЮнионПэй», действующая в соответствии с законодательством РФ и Правилами.

**Платежная клиринговая позиция**

Суммы денежных средств, которые должны быть списаны или зачислены с Расчетного счета.

**Платежный клиринговый центр**

Юридическое лицо, предоставляющее платежные клиринговые услуги в соответствии с Законом о НПС.

**Показатели БФПС**

Показатели БФПС, определенные в пункте 5.11.7 (*Показатели БФПС*) настоящих Правил. Показатели П1, П2, П3, П4 и П5 также определены в пункте 5.11.7 (*Показатели БФПС*) настоящих Правил.

**Положение 266-П**

Положение Банка России от 24 декабря 2006 г. № 266-П «Об эмиссии банковских карт и об операциях, совершаемых с использованием платежных карт».

**Положение 382-П**

Положение Банка России от 9 июня 2012 г. № 382-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».

**Положение 383-П**

Положение Банка России от 19 июня 2012 г. № 383-П «О правилах осуществления перевода денежных средств».

**Положение 607-П**

Положение Банка России о 3 октября 2017 года N 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».

**Пополнение Карты**

Операция с использованием Карты UnionPay, результатом которой является внесение наличных денежных средств на банковский счет Получателя или увеличение остатка электронных денежных средств Получателя.

**Постановление 584**

Постановление Правительства РФ от 13 июня 2012г. № 584 «Положение о защите информации в платежных системах».

**Правила**

В настоящем документе, если прямо не предусмотрено иное, термин «правила платежной системы» означает настоящие Правила.

**Правила НСПК**

Правила НСПК, которые регулируют предоставление операционных и платежных клиринговых услуг НСПК в соответствии со статьей 30.6(4) Закона о НПС, принятые НСПК и опубликованные в публичном доступе в сети Интернет по адресу http://www.nspk.ru/.

В случае противоречий между настоящими Правилами или Стандартами UnionPay, с одной стороны, и Правилами НСПК, с другой стороны, последние имеют преимущественную силу в отношении осуществления НСПК функций Операционного центра и Платежного клирингового центра в соответствии со статьей 30.6 (4) Закона о НПС, который устанавливает, что НСПК предоставляет операционные и платежные клиринговые услуги в соответствии с Правилами НСПК; в отношении других вопросов настоящие Правила и Стандарты UnionPay имеют преимущественную силу.

**Правовой риск**

Риск оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию таких услуг, вследствие несоблюдения Субъектами платежной системы требований законодательства РФ, Правил, договоров, заключенных между Субъектами платежной системы, документов Оператора платежной системы и документов Операторов услуг платежной инфраструктуры либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве РФ, нормативных актах Банка России, Правилах и договорах, заключенных

между Субъектами платежной системы, а также вследствие нахождения Операторов услуг платежной инфраструктуры и Участников под юрисдикцией различных государств.

**Профили рисков**

Профили рисков в значении Приложения 2 к Положению 607-П.

**Прямой участник**

Операторы по переводу денежных средств, включая операторов электронных денежных средств, организаторы торговли, осуществляющие деятельность в соответствии с Федеральным законом от 21 ноября 2011 года N 325-ФЗ «Об организованных торгах», профессиональные участники рынка ценных бумаг, клиринговые организации, юридические лица, являющиеся участниками организованных торгов, и (или) участниками клиринга, и (или) центральным контрагентом в соответствии с Федеральным законом от 7 февраля 2011 года N 7-ФЗ "О клиринге, клиринговой деятельности и центральном контрагенте" (при осуществлении ими переводов денежных средств по сделкам, совершенным на организованных торгах), страховые организации, осуществляющие обязательное страхование гражданской ответственности в соответствии с законодательством Российской Федерации (при осуществлении ими расчетов по обязательным видам страхования гражданской ответственности, предусмотренным законодательством Российской Федерации), международные финансовые организации, иностранные центральные (национальные) банки, иностранные банки (иностранные кредитные организации) и органы Федерального казначейства.

Участники платежной системы, соответствующие критериям, предъявляемым к Прямым участникам, перечисленным в пункте 2.1.1. (*Критерии участия*) и 2.1.2 (*Категории участников*) Правил.

**Распоряжение Платежного клирингового центра**

Сообщение, направляемое Платежным клиринговым центром в Расчётный центр, содержащее реестр нетто-позиций.

**Расчетный счет**

Банковский счет, открытый Прямым участником в Расчетном центре.

**Расчетный центр**

Лицо, предоставляющее расчетные услуги в соответствии с Законом о НПС.

**Регламент выполнения процедур**

Термин имеет значение, определенное в пункте 5.11.7 (*Показатели БФПС*) настоящих Правил.

**Реестр нетто-позиций**

Сообщения, направляемые НСПК в Банк России, включая Платежные клиринговые позиции, выраженные в рублях на нетто-основе, определенные НСПК, и иная информация.

**Риск ликвидности**

Риск оказания услуг платежной инфраструктуры, не соответствующих требованиям к оказанию таких услуг, вследствие отсутствия у Участников денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами платежной системы.

**Риск-событие**

Риск-событие в значении Приложения 2 к Положению 607-П.

**Сводный отчет Расчетного центра**

XML извещение об исполнении, направляемое Расчётным центром в электронном виде через Платежный клиринговый центр.

**Субъекты платежной системы**

Совместно Операторы услуг платежной инфраструктуры, Оператор платежной системы и Участники, соответственно Субъект платежной системы означает любое из перечисленных лиц.

**ТСП (торгово-сервисное предприятие)**

Юридическое лицо или индивидуальный предприниматель, заключившее с Эквайрером соглашение о приеме к оплате Карт UnionPay.

**Участники**

Организации, указанные в п. 1 ч. 1 ст. 21 Закона о НПС, которые присоединились к Правилам путем подписания соглашения (договора) о присоединении с Оператором платежной системы. Присоединение Участников к Правилам может происходить только путем принятия Правил в целом.

**Центральный платежный клиринговый контрагент**

Платежный клиринговый центр, выступающий в соответствии с Законом о НПС плательщиком и получателем средств по переводам денежных средств Участников.

**Эквайрер**

Участник, осуществляющий эквайринг по операциям с Картами UnionPay.

**Электронный файл распоряжений**

Реестр нетто-позиций, оформленный в электронном виде.

**Эмитент**

Участник, занимающийся выпуском Карт UnionPay.

**UnionPay International**

UnionPay International Co., Ltd., компания, учрежденная в соответствии с законодательством Китайской Народной Республики, зарегистрированная по адресу: Китайская Народная Республика, Шанхай, Pudong New, Dongfang Road, дом 6, этажи 2-7.

# Глава 1. Общие положения

## 1.1. Обязательная юридическая сила

Правила имеют обязательную юридическую силу для Оператора платежной системы, Операторов услуг платежной инфраструктуры, а также для всех Прямых участников и Косвенных участников.

## 1.2. Соответствие требованиям

Операторы услуг платежной инфраструктуры и Участники должны соблюдать Правила и законодательство РФ и несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств по Правилам в соответствии с положениями Правил.

## 1.3. Внесение изменений в Правила

Оператор платежной системы вправе в одностороннем порядке вносить изменения в Правила в следующем порядке.

Проект изменений Правил будет опубликован в операционном бюллетене, где с ним могут ознакомиться Операторы услуг платежной инфраструктуры и Участники. Операторы услуг платежной инфраструктуры и Участники вправе направлять Оператору платежной системы свои комментарии к проекту изменений в течение одного месяца с даты публикации соответствующего операционного бюллетеня по адресу, указанному в бюллетене. Дата вступления изменений в силу указывается в самой публикации и должна наступать не менее, чем через два месяца после публикации бюллетеня (один месяц дается на предоставление комментариев на предлагаемые изменения и один месяц должен пройти между окончанием срока для предоставления комментариев и вступления изменений в силу).

В течение десяти календарных дней после вступления в силу изменений к Правилам, Оператор платежной системы направляет такие изменения к Правилам в Банк России для проверки их на соответствие требованиям Закона о НПС.

### 1.4. Конфиденциальная информация

Операторы услуг платежной инфраструктуры и Участники обязуются:

- обрабатывать и хранить конфиденциальную информацию под своим контролем и на условиях строгой конфиденциальности в соответствии с законодательством РФ;
- устанавливать и поддерживать эффективные меры защиты конфиденциальной информации от несанкционированного доступа или использования;
- раскрывать конфиденциальную информацию исключительно тем своим сотрудникам и (или) третьим лицам, которым данная информация необходима для выполнения своих должностных обязанностей.

В дополнение к обязательствам по соблюдению конфиденциальности информации, указанным выше, Операторы услуг платежной инфраструктуры и Участники также обязуются соблюдать требования статьи 10 (1) Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» и статьи 26 Закона о НПС. При этом, требования законодательства РФ накладывают дополнительные ограничения, не противоречащие Правилам в отношении конфиденциальной информации, предоставленной Операторам услуг платежной инфраструктуры и Участникам в рамках Платежной системы.

### 1.5. Порядок осуществления контроля за соблюдением Правил и право на проведение аудита

Оператор платежной системы вправе:

- Проводить аудит документации и процедур любого Оператора услуг платежной инфраструктуры, Участника или ТСП (и относящихся к ним третьих лиц, имеющих отношение к деятельности и продуктам, связанным с Картами UnionPay).
- В любое время проводить проверку, в том числе на объектах Операторов услуг платежной инфраструктуры, Участника, ТСП и относящихся к ним третьих лиц.
- Осуществлять контроль за соблюдением Правил Участниками и Операторами услуг платежной инфраструктуры и налагать штрафы за их несоблюдение.

Порядок осуществления контроля за соблюдением Правил и осуществления аудита в отношении Банка России и НСПК регулируется законодательством и соответствующими договорами между Оператором платежной системы и соответствующими Операторами услуг платежной инфраструктуры.

Процедуры контроля соблюдения Правил включают предварительный и последующий контроль:

1) Предварительный контроль. Оператор платежной системы в письменной форме информирует Участника или Оператора услуг платежной инфраструктуры о планах проверки за соблюдением Правил с указанием их конкретных элементов, по соблюдению которых будет проводиться проверка. Проведение предварительного контроля не требует оснований для ее проведения в виде подозрения в несоблюдении каких-либо положений Правил.

2) Последующий контроль. Любое лицо может проинформировать Оператора платежной системы о подозрении относительно возможного несоблюдения тем или иным Участником или Оператором услуг платежной инфраструктуры Правил. Заявление о несоблюдении представляется Оператору платежной системы в письменной форме и должно содержать достаточно информации для проведения расследования. В течение трех месяцев после получения такого заявления Оператор платежной системы может в письменной форме обратиться к соответствующему Участнику или Оператору услуг платежной инфраструктуры, к которому относится такое заявление, если сочтет, что это заявление о несоблюдении является обоснованным. Участник и (или) Оператор услуг платежной инфраструктуры будет иметь возможность дать разъяснения, которые представляются в письменной форме в течение 30 календарных дней после получения письменного уведомления от Оператора платежной системы, в котором описывается соответствующее нарушение.

При проведении предварительного или последующего контроля соблюдения, в случае подтверждения факта несоблюдения, Участник или Оператор услуг платежной инфраструктуры обязан устранить такой факт несоблюдения. По результатам проведенной проверки Оператор платежной системы может применить в отношении нарушающего лица санкции за несоблюдение Правил в соответствии с положениями Правил. Регулярные или существенные нарушения могут привести к прекращению участия Участника или расторжению договора с Оператором услуг платежной инфраструктуры.

Оператор платежной системы вправе осуществлять дистанционный контроль Участников и Операторов услуг платежной инфраструктуры. Дистанционный контроль представляет собой сбор и анализ публично доступной информации на сайтах Банка России, Операторов услуг платежной инфраструктуры, Участников; мониторинг реестров финансового положения Субъектов платежной системы, новостей касательно отзыва лицензии и иных существенных фактов; устные опросы Субъектов платежной системы.

### 1.6. Штрафные санкции за нарушение Правил

За нарушения Правил Оператор платежной системы может применить механизмы и меры принудительного характера, предусмотренные в Правилах, такие как штрафы и взыскания.

Ниже перечислены санкции, которые применяются дополнительно к любым другим санкциям, предусмотренным Правилами.

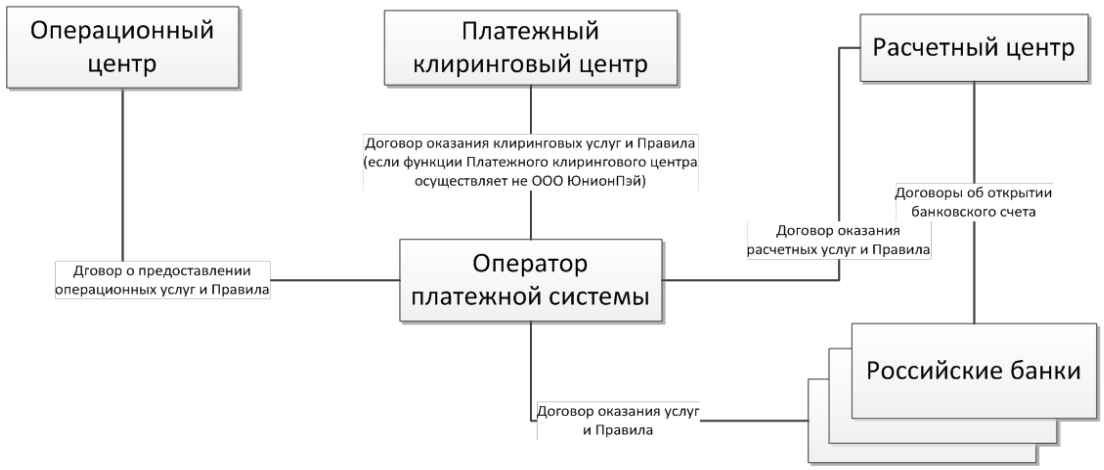
| Нарушение | Санкция |
|---|---|
| Первое нарушение Правил | Предупреждение с указанием срока для устранения нарушения |
| Второе нарушение тех же Правил в течение 12 месяцев после предупреждения о первом нарушении | Штраф в размере, эквивалентном 5 000 долл. США |

| | |
|---|---|
| Третье нарушение тех же Правил в течение 12 месяцев после предупреждения о первом нарушении | Штраф в размере, эквивалентном 10 000 долл. США |
| Четыре или более нарушений тех же Правил в течение 12 месяцев после предупреждения о первом нарушении | На усмотрение Оператора платежной системы |

Все штрафы, указанные в настоящем разделе, начисляются и оплачиваются в российских рублях по курсу обмена долларов США на российские рубли, публикуемому в сети Интернет на сайте www.unionpayintl.com на дату начисления соответствующего штрафа.

### 1.7. Порядок взаимодействия между Оператором платежной системы, Участниками и Операторами услуг платежной инфраструктуры

Если в Правилах не установлено иное, Оператор платежной системы, Участники и Операторы услуг платежной инфраструктуры взаимодействуют, как проиллюстрировано и описано ниже.




1. Эквайрер направляет Эмитенту авторизационный запрос на осуществление перевода денежных средств при поддержке Операционного центра. Эмитент отвечает на авторизационный запрос акцептом или отказом. В случае акцепта Эмитента Эквайрер направляет клиринговый файл с записью такой операции по переводу денежных средств для клиринга в Операционный центр, который переправляет его в Платежный клиринговый центр
2. Платежный клиринговый центр осуществляет платежный клиринг в соответствии с разделом 6.3 Правил. Платежный клиринговый центр информирует Прямых участников об их платежных клиринговых позициях, отправленных на исполнение в Расчетный центр.
3. Расчетный центр осуществляет перевод денежных средств по счетам Участников на основании распоряжений Участников, поступивших от Платежного клирингового центра.

### 1.8. Взаимодействие с иными платежными системами

Взаимодействие с иными платежными системами не осуществляется.

### 1.9. Выпуск совместных карт

Оператор платежной системы вправе договориться с операторами иных платежных систем о

выпуске совместных (кобрендовых) банковских карт.

Для эмиссии совместных банковских карт, Эмитент должен быть участником обеих платежных систем – Платежной системы и иной платежной системы, совместно с которой осуществляется выпуск совместной банковской карты.

К эмиссии совместных банковских карт применяются операционные и технические требования UnionPay. При эмиссии совместных банковских карт используется БИН UnionPay.

При совершении операций по совместным банковским картам через Платежную систему, такие операции регулируются Правилами.

# Глава 2. Участие в системе, выход и прекращение действия

## 2.1. Участие в системе

Участниками могут быть только организации, указанные в статье 21 Закона о НПС.

### 2.1.1. Критерии участия

**Прямой участник**

Для участия в Платежной системе в качестве Прямого участника заявитель, а также Участник на протяжении всего периода участия в Платежной системе должны соответствовать следующим критериям:

- иметь необходимые разрешения/лицензии, действующие договоры и корпоративные одобрения, необходимые для осуществления деятельности в рамках платежной системы, включая деятельность по переводу денежных средств;
- обладать финансовой устойчивостью, исключающей возможность инициирования процедуры несостоятельности (банкротства);
- соответствовать требованиям, установленным в Законе о НПС и Правилах;
- соблюдать требования и осуществлять меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- соблюдать требования в отношении информационной безопасности, банковской тайны и защиты данных;
- соответствовать техническим и иным требованиям, предусмотренным Правилами;
- иметь систему управления рисками, соответствующую требованиям Правил, о чем Оператор платежной системы выдает положительное заключение;
- заключить соглашение (договор) с Оператором платежной системы о присоединении к Платежной системе, неотъемлемой частью которого являются Правила;
- надлежащим образом исполнять обязательства, установленные Правилами и соглашением (договором) о присоединении к Платежной системе;
- иметь возможность открытия банковского счета в Расчетном центре и соблюдать стандарты проведения расчетов в целях обеспечения бесперебойности функционирования Платежной системы.

Помимо этого, для участия в Платежной системе в качестве Прямого участника заявитель, а также Участник на момент вступления в Платежную систему должны иметь или находиться в процессе получения лицензии участника UnionPay International (любой из видов членства: Принципиальное членство, Сетевое членство, Аффилированное членство или статус Члена-участника);

Датой начала участия в Платежной системе является дата начала действия соглашения (договора) с Оператором платежной системы о присоединении к Платежной системе.

В связи с тем, что Банк России является Расчетным центром, Прямые участники обязаны заключить дополнительные соглашения с Банком России к договорам банковского счета, предусматривающие следующее:

- осуществление расчетных услуг Банком России;
- осуществление Банком России функций Центрального платежного клирингового контрагента и расчетного центра по осуществляемым на территории РФ переводам денежных средств, не являющимся трансграничными, с использованием международных платежных карт;
- исполнение обязательства по возмещению, т.е. обязательства Участника по переводу Банку России денежных средств в сумме непокрытой позиции и штрафа за непокрытую позицию.

В связи с тем, что НСПК является Операционным центром и Платежным клиринговым центром, Прямые участники должны присоединиться к Правилам НСПК (с учетом установленных НСПК сроков, указанных в Правилах НСПК), а также обеспечить подключение к НСПК.

**Косвенный участник**

Для участия в Платежной системе в качестве Косвенного участника заявитель, а также Участник на протяжении всего периода участия в Платежной системе должны соответствовать следующим критериям:

- иметь необходимые разрешения/лицензии, действующие договоры и корпоративные одобрения, необходимые для осуществления деятельности в рамках платежной системы;
- соответствовать требованиям, установленным в Законе о НПС и Правилах;
- соблюдать требования и осуществлять меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма;
- соблюдение требований в отношении информационной безопасности, банковской тайны и защиты данных;
- соответствовать техническим и иным требованиям, предусмотренным Правилами;
- подключаться к Платежной системе через Прямого участника;
- заключить с Оператором платежной системы договор присоединения к Платежной системе, неотъемлемой частью которого являются Правила;
- надлежащим образом исполнять обязательства, установленные Правилами и договором о присоединении к Платежной системе.

Прямой участник, через которого подключается Косвенный участник, несет полную ответственность за действия (бездействия) Косвенного участника перед Оператором платежной системы.

### 2.1.2. Категории участников

Участник может быть Прямым участником или Косвенным участником.

**Прямой участник.** Прямой участник заключает договор с Оператором платежной системы о присоединении к Платежной системе. Правила являются неотъемлемой частью такого договора. Прямой участник должен открыть банковский счет в Расчетном центре. Прямые участники осуществляют подготовку необходимых отчетов в рамках работы с платежными продуктами UnionPay, предусмотренных Правилами. Прямые участники несут полную ответственность за выполнение всех финансовых обязательств перед Оператором платежной системы, возникающих в рамках работы в Платежной системе, в связи с чем Оператор платежной системы проводит оценку их необходимого и достаточного финансового состояния и внутренних процессов по соблюдению данного требования.

Для обеспечения бесперебойности работы связи, Прямой участник должен использовать поставщиков услуг связи, предоставляющих не менее двух каналов связи разных операторов связи (основной и резервный каналы связи, между которыми должен быть обеспечен автоматический переход. Для чиповых карт должен применяться EMV-совместимый стандарт UICS. Для мониторинга поддержки работы системы должен быть гарантирован онлайн сервис, работающий в круглосуточном режиме без выходных. Для обеспечения защиты информации необходимо использовать иерархическое шифрование. Для шифрования персонального ПИН-кода должен быть использован аппаратный модуль шифрования. ПИН-код должен быть зашифрован на протяжении всего цикла передач. Участники должны иметь и регулярно обновлять документацию по методам и способам защиты данных.

Взаимодействие прямых участников с Партнерами.

Прямые участники могут заключать партнерские соглашения (договоры) с Партнерами для осуществления переводов денежных средств и последующих расчетов по операциям с использованием Карт UnionPay на территории Российской Федерации без участия Оператора платежной системы в качестве стороны такого договора. Взаимодействие Прямых участников с Партнерами осуществляется с учетом следующего:

- заключение и исполнение партнерских соглашений (договоров) Прямыми участниками не должно противоречить требованиям настоящих Правил и требованиям законодательства Российской Федерации, в том числе нормативным актам Банка России;

- Прямые участники обязаны по требованию Оператора платежной системы незамедлительно предоставить всю запрашиваемую информацию о заключенных партнерских соглашениях (договорах) и порядке их исполнения;

- распоряжения на перевод денежных средств Партнеров включаются в платежную клиринговую позицию соответствующего Прямого участника; и

- Оператор платежной системы и Операторы услуг платежной инфраструктуры не несут ответственности перед Прямым участником за его убытки и потери Прямого

участника, возникшие в результате заключения и/или неисполнения последним соответствующего договора с Партнером.

**Косвенный участник**. Косвенный участник заключает договор с Оператором платежной системы о присоединении к Платежной системе. Правила являются неотъемлемой частью такого договора. Косвенный участник должен открыть банковский счет у Прямого участника в целях проведения расчетов с другими Участниками. Каждый Косвенный участник должен заключить соглашение с Прямым участником-спонсором, который будет полностью отвечать за него перед Оператором платежной системы. Прямой участник должен подтвердить Оператору платежной системы свое спонсорство над Косвенным участником.

### 2.2. Использование Идентификационного номера учреждения (ИНУ)

После утверждения заявителя в качестве Участника, Оператор платежной системы присваивает Участнику уникальный Идентификационный номер учреждения (ИНУ) для обеспечения однозначной идентификации каждого Участника и формы его участия в Платежной системе (прямое или косвенное участие).

ИНУ изымается из реестра активных ИНУ после того, как Участник прекращает свое участие в Платежной системе.

### 2.3. Временное приостановление

Правила не устанавливают критерии для временного приостановления участия.

### 2.4. Прекращение участия в платежной системе

Участие в Платежной системе может быть прекращено (i) по инициативе Участника, (ii) по инициативе Оператора платежной системы, а также (iii) автоматически при наступлении событий, определенных Правилами.

1. Прекращение участия по инициативе Участника. Участник, желающий прекратить участие в Платежной системе, направляет Оператору платежной системы уведомление в письменной форме не менее чем за 180 (сто восемьдесят) дней до желаемой даты прекращения участия. Участие в Платежной системе считается прекращенным с даты, указанной в таком письменном уведомлении. В том случае, если дата прекращения участия в Платежной системе в уведомлении не указана, участие в Платежной системе прекращается через 180 (сто восемьдесят) дней после даты получения UnionPay письменного уведомления.

2. Прекращение участия по инициативе Оператора платежной системы. Участие в Платежной системе может быть прекращено по инициативе Оператора платежной системы в следующих случаях: (i) несоответствие Участника критериям участия, установленным в Правилах (за исключением критерия наличия лицензии участника UnionPay International); (ii) неисполнение или ненадлежащее исполнение Участником своих обязательств, а также иное умышленное или неоднократное нарушение Участником Правил и (или) соглашения о присоединении к Платежной системе; (iii) инициирование в отношении Участника процедуры несостоятельности (банкротства) либо изменение финансового состояния Участника, которое может повлечь признание Участника несостоятельным (банкротом). Участие прекращается по единоличному усмотрению Оператора платежной системы путем отправки Участнику уведомления. Участие прекращается с момента доставки или попытки вручения такого уведомления по адресу Участника, известному Оператору платежной системы, даже если фактическое получение не состоялось по какой-либо причине.

3. Автоматическое прекращение участия. Участие в Платежной системе прекращается автоматически в случае признания Участника несостоятельным (банкротом) или в случае начала процесса ликвидации, а также иных случаях прекращения деятельности Участника либо невозможности осуществления деятельности вследствие решения уполномоченного государственного органа (включая случаи отзыва лицензии на осуществление переводов денежных средств, а также иной деятельности в рамках Платежной системы). Участник обязан в течение одного рабочего дня уведомить Оператора платежной системы о наступлении событий, указанных в настоящем пункте и о прекращении своего участия в Платежной системе. В случае если Оператор платежной системы сам узнает о наступлении соответствующих событий, он отправляет Участнику уведомление, подтверждающее, что его участие в Платежной системе прекратилось.

4. Прекращение участия Участника с Непокрытой позицией по инициативе Оператора платежной системы. Участие в Платежной системе Участника с Непокрытой позицией может быть прекращено в любой момент в период существования такой Непокрытой позиции. Условия, процедура, последствия такого прекращения установлены в разделе 6.3 «*Осуществление платежного клиринга и расчетов в Платежной системе*» Правил.

## 2.5. Последствия прекращения участия в платежной системе

За исключением случаев, когда в Правилах и (или) соглашении о присоединении к Платежной системе предусмотрено иное, Участник, выбывающий из Платежной системы, утрачивает все права Участника и перестает нести обязательства Участника (за исключением обязательств по соблюдению конфиденциальности) с даты прекращения участия в Платежной системе.

За исключением случаев, когда в Правилах и (или) соглашении о присоединении к Платежной системе предусмотрено иное, в случае прекращения участия в Платежной системе:

- выбывающий Участник обязуется незамедлительно прекратить осуществление любой деятельности, связанной с Картами UnionPay, право на осуществление которой было ему предоставлено в соответствии с Правилами и соглашением о присоединении к Платежной системе;
- комиссии/сборы, выплаченные выбывающим Участником Оператору платежной системы до прекращения участия в Платежной системе, возмещению не подлежат;
- выбывающий Участник продолжает нести ответственность по долгам и другим обязательствам, возникшим до прекращения участия в Платежной системе, включая обязательства по любым незавершенным операциям;
- выбывающий Участник обязуется оказывать Оператору платежной системы содействие в осуществлении формальных процедур, связанных с прекращением его участия в Платежной системе;
- выбывающий Участник обязуется не заниматься никакой деятельностью, в результате осуществления которой у неограниченного круга лиц может возникнуть ложное представление о том, что он вправе осуществлять деятельность, связанную с Картами UnionPay; и
- выбывающий Участник обязуется принять все необходимые меры в целях прекращения деятельности, связанной с Картами UnionPay, и недопущения создания представления о том, что он по-прежнему вправе осуществлять деятельность, связанную с Картами UnionPay. В частности, выбывающий Участник обязуется направить соответствующие уведомления всем сторонам, которых может затронуть прекращение им деятельности, связанной с Картами UnionPay, и расторгнуть соответствующие соглашения.

# Глава 3. Обработка операций

## 3.1. Порядок проведения операции

Карты UnionPay позволяют Держателям карты производить платежи или покупки без использования наличных денежных средств, снимать наличные в банкоматах и в отделениях банков, производить платежи в ТСП и зачислять денежные средства на Карту UnionPay или переводить на счет другого лица, осуществлять P2P Операции, получать денежные средства в рамках Перевода с Карты на Карту, а также совершать иные платежные операции.

В типичной операции по оплате товаров и услуг по Карте UnionPay участвуют четыре стороны: Держатель карты, ТСП, Эмитент и Эквайрер. Типичная операция покупки показана на следующей схеме:


Для начала типичной операции Держатель карты приобретает товары или услуги у ТСП, с использованием Карты UnionPay или иного платежного средства. ТСП отправляет Эмитенту запрос авторизации через Операционный центр. Запрос авторизации содержит информацию, которая позволяет Эмитенту одобрить или отклонить операцию. Запрос авторизации может содержать данные ПИН, которые Эмитент может проверить и, таким образом, удостовериться, что лицо, осуществляющее операцию, является правомочным Держателем карты. После авторизации операции Эмитентом Эмитент направляет запрос Оператору платежной системы и перечисляет Эквайреру с использованием процедуры расчетов сумму, равную сумме операции, и вычитает сумму операции из средств, предоставленных Держателем карты, или иным образом проводит операцию по Карте UnionPay. Эквайрер компенсирует расходы Эмитента по выпуску Карт UnionPay посредством уплаты межбанковской комиссии в процессе расчетов. Эквайрер оплачивает ТСП сумму покупки за вычетом сбора за обслуживание торговых точек. Эмитенты и Эквайреры могут привлекать третьих лиц для оказания им содействия в их деятельности в качестве Участника, включая такие виды деятельности как подготовка выписок по Картам UnionPay, привлечение подходящих ТСП и направление запросов на авторизацию операций. Эквайреры обязаны предоставить ТСП (или обеспечивают, чтобы ТСП были предоставлены) материалы, необходимые для обработки операций. Эмитент может применять различные методы проверки перед авторизацией операции. Эмитент может сравнить запрос авторизации с другими запросам авторизации по той же Карте UnionPay и таким образом определить вероятность того, что операция является мошеннической. Эмитент также имеет возможность проверить достаточность средств у Держателя карты для осуществления операции. На основании проведенной им оценки возможности Держателя карты оплатить операцию и иных факторов,

Эмитент либо авторизует запрос, либо отклонит запрос авторизации. Если Эмитент одобряет запрос авторизации, Карта UnionPay может использоваться для завершения операции.

## 3.2. Порядок предоставления Участниками и Операторами услуг платежной инфраструктуры информации Оператору платежной системы

### 3.2.1. Предоставление информации Участниками

С учетом применимых законов и нормативных актов, Участник обязан в письменной форме предоставлять Оператору платежной системы по его запросу следующую статистическую информацию о деятельности и продуктах, связанных с Картами UnionPay:

- количество и адреса ТСП, принимающих к оплате Карты UnionPay;
- количество и адреса банкоматов;
- количество выпущенных Карт UnionPay, в том числе информацию о количестве активных и неактивных карт; и
- объем операций и средняя сумма одной операции.

Такая представленная Участником информация будет использована UnionPay в качестве конфиденциальной информации для справочных целей, а также для развития и продвижения деятельности, связанной с Картами UnionPay. В некоторых случаях такая информация может использоваться для расчета ставки комиссионного сбора за услуги.

Участники обязаны информировать Оператора платежной системы о спорах, нестандартных и чрезвычайных ситуациях, в том числе о сбоях в работе системы и результатах расследований, в том числе, их причинах и последствиях, по мере возникновения таковых.

В любое время по письменному запросу Оператора платежной системы Участники обязаны предоставлять и иную информацию по любым вопросам, регулируемым Правилами и связанным операциями по Картам UnionPay. В запросе будет указана дата, к которой должна быть представлена соответствующая информация (такая дата должна наступать не раньше тридцати календарных дней после даты запроса). Запрашиваемая информация предоставляется в письменном виде и направляется в адрес, указанный в запросе.

Участники обязаны немедленно сообщить Оператору платежной системы обо всех возможных или подтвержденных случаях потери, кражи или подделки любой конфиденциальной информации, содержащей данные о счетах и операциях по Картам UnionPay.

Участники не обязаны предоставлять информацию, раскрытие которой, по мнению юридического консультанта Оператора платежной системы, может привести к возникновению у Оператора платежной системы и (или) Участника(ов) существенных юридических рисков.

Если, по мнению Участника, запрашиваемая информация является конфиденциальной, Оператор платежной системы должен обрабатывать такую информацию со степенью заботливости, которую юридический консультант Оператора платежной системы сочтет целесообразной.

Каждый Участник обязан обеспечить соблюдение им Правил и применимого законодательства в части раскрытия Оператору платежной системы любых данных по операциям по Картам UnionPay и иной информации, включая законодательство, требующие от Участника уведомить физических лиц о правилах обработки информации и получить согласие таких физических лиц в отношении такой обработки. Участники должны получить

согласие Держателей карт на обработку и передачу, в том числе трансграничную, персональных данных Участникам/Оператору платежной системы/Операторам услуг платежной инфраструктуры и их аффилированным лицам (включая компании ООО «ЮнионПэй», UnionPay International, China UnionPay и иным (включая компании ООО «ЮнионПэй», UnionPay International, China UnionPay и иным компаниям группы UnionPay). Участники должны предоставить Оператору платежной системы копии соответствующих согласий Держателей карт по запросу Оператора платежной системы. Участники должны возместить Оператору платежной системы (и любой иной компании группы UnionPay, которой были переданы персональные данные Держателя карты) любой ущерб, возникший вследствие того, что соответствующий Участник не получил в надлежащем порядке согласие Держателя карты на передачу персональных данных. В случае проведения расследования в связи с нарушением Правил, Участник обязан ответить Оператору платежной системы и предоставить любую требуемую информацию в указанный Оператором платежной системы срок по почте, через курьерскую службу доставки, по факсу, лично в руки, по электронной почте или с помощью других электронных средств связи. Ответ на уведомление считается действительным, если он отправлен или передан Оператору платежной системы Участником и фактически получен.

### 3.2.2. Предоставление информации Оператором услуг платежной инфраструктуры

В любое время по запросу Оператора платежной системы Операционный центр, Платежный клиринговый центр и Расчетный центр обязаны в письменной форме предоставлять ему информацию о платежных операциях с Картами UnionPay, которая касается выполнения ими операционных, клиринговых и расчетных функций, соответственно. В запросе о предоставлении информации должна быть указана дата, до которой требуется предоставить указанную информацию, (такая дата должна наступать не раньше тридцати календарных дней после даты запроса). Запрашиваемая информация должна быть предоставлена в письменном виде по адресу, указанному в запросе.

Операционный центр обязан ежедневно предоставлять Оператору платежной системы информацию по операциям и информацию о чрезвычайных ситуациях или об исключительных случаях – немедленно по наступлении таковых.

Платежный клиринговый центр и Расчетный центр обязаны предоставлять Оператору платежной системы данные и прочую информацию по его запросу.

Порядок предоставления информации Банком России и НСПК регулируется законодательством и соответствующими договорами между Оператором платежной системы и соответствующими Операторами услуг платежной инфраструктуры.

При этом Оператор платежной системы не несет ответственности, если невозможность получения информации Оператором платежной системы привела к неблагоприятным последствиям для Субъектов платежной системы (убытки и т.д.).

## 3.3. Платежная система: роль и функции

Оператор платежной системы привлекает Операционный центр, Платежный клиринговый центр и Расчетный центр, отвечающие требованиям Закона о НПС для оказания Участникам операционных услуг, услуг платежного клиринга и расчетных услуг.

В соответствии с Законом о НПС, с 1 января 2016 года в отношении Внутринациональных операций НСПК является Операционным центром и Платежным клиринговым центром, Банк России является Расчетным центром. В соответствии с договорами, заключенными Оператором платежной системы с НСПК и Банком России, Оператор платежной системы не несет

ответственность за выполнение НСПК и Банком России функций, которые они выполняют в рамках указанных договоров (в т.ч. операционные, клиринговые, расчетные функции, координация взаимодействия, передача сообщений и т.д.), перед Участниками и иными лицами.

### 3.3.1. Оператор платежной системы

Оператор платежной системы:

- определяет Правила, организацию Платежной системы и осуществляет контроль за соблюдением Правил Участниками и Операторами услуг платежной инфраструктуры;
- осуществляет контроль за оказанием услуг платежной инфраструктуры Участникам;
- организовывает систему управления рисками Платежной системы в соответствии со статьей 28 Закона о НПС, а также в режиме реального времени осуществляет контроль и управление рисками Платежной системы, за исключением рисков, управление которыми осуществляется АО «НСПК» и Банком России (подробное описание процедуры управления рисками приведено в главе 5 Правил);
- ведет список Операторов услуг платежной инфраструктуры и привлекает Операторов услуг платежной инфраструктуры в соответствии с Законом о НПС.

Перечень Операторов услуг платежной инфраструктуры направляется Оператором платежной системы в Банк России вместе с регистрационным заявлением на регистрацию в качестве Оператора платежной системы в порядке и форме, установленном Банком России. В случае привлечения новых Операторов услуг платежной инфраструктуры или расторжения существующих договоров, Оператор платежной системы направляет обновленный перечень Операторов услуг платежной инфраструктуры в Банк России в течение 10 календарных дней с момента изменения перечня.

### 3.3.2. Операторы услуг платежной инфраструктуры

В соответствии с Законом о НПС Операторы услуг платежной инфраструктуры обязаны обеспечивать конфиденциальность информации и безопасность передачи данных, в том числе соблюдать требования о средствах и методах обеспечения информационной безопасности в соответствии с Правилами, Федеральным законом от 02.12.1990 «О банках и банковской деятельности», Постановлением 584, Положением 382-П и иными применимыми нормативно-правовыми актами РФ.

Операторы услуг платежной инфраструктуры должны быть в состоянии обеспечить БФПС в соответствии с Правилами и иметь достаточную финансовую ликвидность для выполнения своих функций.

### 3.3.3. Операционный центр

Операционным центром в Платежной системе выступает НСПК в соответствии с законом о НПС. Операционный центр обеспечивает в рамках Платежной системы:

- доступ к услугам по переводу денежных средств, в том числе с использованием электронных средств платежа;
- обмен электронными сообщениями между Участниками, а также между Участниками и их клиентами, Платежным клиринговым центром и Расчетным центром; и между Платежным клиринговым центом и Расчетным центром.

Операционный центр обязан не разглашать третьим лицам информацию об операциях, в том числе о сумме операций, номере счета и другую связанную с этим информацию, если иное прямо не предусмотрено законодательством РФ.

Операционный центр несет ответственность за реальный ущерб, причиненный Участникам и Расчетному центру в результате неоказания (или ненадлежащего оказания) операционных услуг.

Операционный центр несет ответственность перед Расчетным центром и Оператором платежной системы вследствие неоказания (ненадлежащего оказания) операционных услуг в соответствии с законодательством и соответствующими договорами, заключенными между Оператором платежной системы и соответствующими Операторами платежной инфраструктуры.

Операционный центр оказывает услуги непосредственно Участникам. Участники, Оператор платежной системы и Расчетный центр взыскивают убытки, причиненные неоказанием (ненадлежащим оказанием) операционных услуг, напрямую с Операционного центра в соответствии с законодательством и соответствующими договорами, заключенными между Оператором платежной системы и соответствующими Операторами платежной инфраструктуры. Ни при каких обстоятельствах такие требования не могут быть обращены к Оператору платежной системы (в том числе в порядке регресса).

Операционный центр должен иметь резервные мощности, посредством которых он мог бы предоставить все необходимые услуги в случае выхода из строя основных мощностей, и обеспечивает непрерывность оказания операционных услуг в соответствии с законодательством РФ.

В целях обеспечения бесперебойного оказания услуг платежной инфраструктуры Участникам Операционный центр помимо выполнения иных требований, установленных в настоящих Правилах, должен также выполнять следующие требования:

- иметь фактическую и юридическую возможность осуществлять свою деятельность (т.е. деятельность Операционного центра не должна быть прекращена или приостановлена);
- иметь все лицензии и разрешения, а также действующие договоры, необходимые для оказания операционных услуг и надлежащего осуществления денежных переводов;
- соблюдать показатели бесперебойности оказания операционных услуг, установленные в Правилах;
- соблюдать временной регламент функционирования Платежной системы, установленный в Правилах;
- соблюдать требования к допустимым уровням риска, установленные в Правилах;
- выполнять иные функции, если это предусмотрено действующим законодательством и/или договором, заключенным с Операционным центром.

Операционный центр обязан нести ответственность непосредственно перед Участниками за надлежащее оказание операционных услуг и прочей деятельности, осуществляемой напрямую или опосредованно, в соответствии с законодательством РФ.

В случае несоблюдения установленных требований Операционный центр несет ответственность в соответствии с настоящими Правилами, иными актами Оператора платежной системы, а также действующим законодательством РФ.

### 3.3.4. Платежный клиринговый центр

Платежным клиринговым центром в Платежной системе выступает НСПК в соответствии с Законом о НПС.

Платежный клиринговый центр должен:

- обеспечивать гарантированный уровень бесперебойности и безопасности оказания услуг платежного клиринга;
- осуществлять прием подлежащих исполнению распоряжений Участников для перевода денежных средств в рамках Платежной системы в соответствии с главой 6 Правил;
- определять платежные клиринговые позиции на нетто-основе, включая надлежащее установление параметров расчета платежных клиринговых позиций для каждого Участника;
- передавать Расчетному центру от имени Участников подлежащие исполнению распоряжения Участников в электронном виде в соответствии с положениями главы 6 Правил;
- обеспечивать отправку Участникам подтверждений, касающихся приема к исполнению и исполнения распоряжений Участников;
- нести ответственность непосредственно перед Участниками за надлежащее оказание услуг платежного клиринга и прочей деятельности, осуществляемой напрямую или опосредованно, в соответствии с законодательством РФ;
- осуществлять свою деятельность в соответствии с положениями главы 6 Правил;
- выполнять иные функции, если это предусмотрено действующим законодательством и/или договором, заключенным с Платежным клиринговым центром.

Платежный клиринговый центр несет ответственность за убытки, причиненные Участникам и Расчетному центру вследствие неоказания (ненадлежащего оказания) платежных клиринговых услуг.

Платежный клиринговый центр несет ответственность перед Расчетным центром и Оператором платежной системы вследствие неоказания (ненадлежащего оказания) платежных клиринговых услуг в соответствии с законодательством и соответствующими договорами, заключенными между Оператором платежной системы и соответствующими Операторами платежной инфраструктуры.

Платежный клиринговый центр оказывает услуги непосредственно Участникам. Участники, Оператор платежной системы и Расчетный центр взыскивают убытки, причиненные неоказанием (ненадлежащим оказанием) платежных клиринговых услуг, напрямую с Платежного клирингового центра в соответствии с законодательством и соответствующими договорами, заключенным между Оператором платежной системы и соответствующими Операторами платежной инфраструктуры. Ни при каких обстоятельствах такие требования не могут быть обращены к Оператору платежной системы (в том числе в порядке регресса).

В целях обеспечения бесперебойного оказания услуг платежной инфраструктуры Участникам Платежный клиринговый центр помимо выполнения иных требований, установленных в настоящих Правилах, должен также выполнять следующие требования:

- иметь фактическую и юридическую возможность осуществлять свою деятельность (т.е. деятельность Платежного клирингового центра не должна быть прекращена или приостановлена);
- иметь все необходимые лицензии и разрешения, а также действующие договоры, необходимые для оказания клиринговых услуг и надлежащего осуществления денежных переводов;
- соблюдать показатели бесперебойности оказания клиринговых услуг, установленные в Правилах;
- соблюдать временной регламент функционирования Платежной системы, установленный в Правилах;
- соблюдать требования к допустимым уровням риска, установленные в Правилах.

В случае несоблюдения установленных требований Платежный клиринговый центр несет ответственность в соответствии с настоящими Правилами, иными актами Оператора платежной системы, а также действующим законодательством РФ.

### 3.3.5. Расчетный центр

Расчетным центром в Платежной системе выступает Банк России в соответствии с Законом о НПС.

Расчетный центр должен:

- обеспечивать гарантированный уровень бесперебойности и безопасности оказания расчетных услуг;
- принимать к исполнению от Платежного клирингового центра Реестры нетто-позиций, составленные за каждый клиринговый период;
- при приеме к исполнению Реестра нетто-позиций выполнять процедуры контроля Реестра нетто-позиций;
- составлять распоряжения на основании принятых к исполнению Реестров нетто-позиций;
- осуществлять списание денежных средств в качестве получателя средств с банковских счетов Участников, открытых в Банке России, при выполнении Расчетным центром функций центрального платежного клирингового контрагента и расчетного центра на основании инкассового поручения в размере дебетовых нетто-позиций, указанных в Реестре нетто-позиций;
- осуществлять зачисление денежных средств в качестве плательщика на банковские счета Участников, открытых в Банке России, при выполнении Расчетным центром функций Центрального платежного клирингового контрагента и Расчетного центра в размере кредитовых нетто-позиций, указанных в Реестре нетто-позиций;
- выполнять иные функции, если это предусмотрено действующим законодательством и/или договором, заключенным с Расчетным центром.

Дополнительные условия предоставления операционных услуг, услуг платежного клиринга, а также расчетных услуг могут быть обозначены Оператором платежной системы в соответствующих договорах на предоставление услуг или любых иных договорах. Расчетный центр несет ответственность за неоказание (ненадлежащее оказание)

расчетных услуг Участникам в соответствии с заключенными между ними договорами банковского счета.

Участники взыскивают убытки, причиненные неоказанием (ненадлежащим оказанием) расчетных услуг, напрямую с Расчетного центра. Ни при каких обстоятельствах такие требования не могут быть обращены к Оператору платежной системы.

В целях обеспечения бесперебойного оказания услуг платежной инфраструктуры Участникам Расчетный центр помимо выполнения иных требований, установленных в настоящих Правил, Расчетный центр должен также выполнять следующие требования:

- соблюдать показатели бесперебойности оказания расчетных услуг, установленные в Правилах;
- соблюдать временной регламент функционирования Платежной системы, установленный в Правилах;
- соблюдать требования к допустимым уровням риска, установленные в Правилах.

Расчетный центр обязан нести ответственность непосредственно перед Участниками за надлежащее оказание расчетных услуг и прочей деятельности, осуществляемой напрямую или опосредованно, в соответствии с законодательством РФ.

### 3.3.6. Участники – Роль Эмитента и его обязанности

#### 3.3.6.1. Обязательства по раскрытию информации

Эмитент, руководствуясь Законом о НПС, а также иным применимым законодательством РФ и Правилами, обязан информировать Держателей карт об их правах и о требованиях, предъявляемых к использованию Карт UnionPay.

#### 3.3.6.2. Требования к оказанию услуг

Эмитент обеспечивает обслуживание счета и функционирование службы поддержки карт в чрезвычайных ситуациях в соответствии с Правилами.

#### 3.3.6.3. Мониторинг операции и контроль над рисками

Эмитент осуществляет мониторинг операций и рисков на ежедневной основе. Это касается обязательств по переводу денежных средств, а также наложения ограничений на определенные виды операций, когда при анализе их финансового состояния выявляется повышенный риск. В соответствии с законодательством РФ и другим применимым законодательством, могут быть наложены ограничения в виде ограничения суммы операции, проверки ПИН-кода, географическое расположения места проведения операции и т.д.

### 3.3.7. Участники – Роль и обязанности Эквайрера

#### 3.3.7.1. Обслуживание всех Карт UnionPay

Эквайреры обязаны принимать и обслуживать все Карты UnionPay.

#### 3.3.7.2. Бесперебойность работы системы

Эквайрер обеспечивает круглосуточную работу системы без выходных и осуществляет круглосуточный мониторинг ее работы. Эквайрер обязуется не менее чем за 5 рабочих дней уведомлять Оператора платежной системы о предполагаемом приостановлении онлайн операций. Эквайрер также обязуется своевременно сообщать своим ТСП и другим точкам обслуживания о таком приостановлении. В случае аварийного приостановления

онлайн операций, Эквайрер должен незамедлительно сообщить об этом Оператору платежной системы, своим ТСП и другим точкам обслуживания.

### 3.3.8. Валюта операции и конвертация валюты

#### 3.3.8.1. Валюта операции

На территории РФ операции по Картам UnionPay (эмитируемым на территории РФ) проводятся в валюте РФ за исключением случаев, когда законодательство РФ разрешает осуществлять расчеты в иностранной валюте (например, в случае снятия наличных денежных средств в банкоматах, расчетов в магазинах беспошлинной торговли, а также в иных разрешенных случаях). Платежный клиринговый центр рассчитает сумму платежной клиринговой позиции в валюте РФ. В случае, если валюта операции или валюта карточного счета Карты UnionPay не является валютой РФ, Платежный клиринговый центр использует для расчета платежной клиринговой позиции курс обмена валюты, указанный в пункте 3.3.8.2 Правил.

#### 3.3.8.2. Курс обмена валюты

Обмен валюты между Оператором платежной системы и Участниками осуществляется по курсу, установленному Банком России на момент осуществления соответствующей операции, и опубликованному на официальном сайте Банка России по адресу www.cbr.ru на момент осуществления соответствующей операции.

# Глава 4. Порядок обеспечения безопасности и защиты информации

## 4.1. Общие требования

Оператор платёжной системы, Операторы услуг платежной инфраструктуры, Участники и привлеченные ими лица (в том числе, операторы по переводу денежных средств и банковские платежные агенты (субагенты)) обеспечивают выполнение требований Постановления 584 и Положения 382-П, требования Правил и международных стандартов информационной безопасности в порядке, установленном Правилами, а также обязаны гарантировать банковскую тайну в соответствии с законодательством РФ о банках и банковской деятельности.

Участники и Расчётный центр выполняют и обеспечивают выполнение третьими сторонами, привлечёнными к деятельности по оказанию услуг по переводу денежных средств, требований к обеспечению защиты информации в соответствии с Правилами при осуществлении переводов денежных средств, с учётом перечня выполняемых ими операций и используемых ими автоматизированных систем, программного обеспечения, средств вычислительной техники и телекоммуникационного оборудования.

Оператор платежной системы, Участники и Операторы услуг платежной инфраструктуры самостоятельно определяют порядок обеспечения защиты информации с учетом требований Постановления 584 и Положения 382-П, а также требований Правил и международных стандартов информационной безопасности в соответствии с Правилами. Для проведения работ по обеспечению защиты информации при осуществлении переводов денежных средств Оператор платёжной системы, Участники и Операторы услуг платёжной инфраструктуры вправе привлекать организации, имеющие лицензии на осуществление деятельности по технической защите информации и(или) по разработке и производству средств защиты информации. Оператор платёжной системы вправе привлекать в Платежную систему только тех Участников, которые соблюдают требования Положения 382-П.

Оператор платёжной системы осуществляет контроль за соблюдением Участниками и привлеченными ими третьими лицами требований Правил в части защиты информации.

Требования к обеспечению защиты информации при осуществлении переводов денежных средств применяются для обеспечения защиты следующей информации:

- информации об остатках денежных средств на банковских счетах;
- информации о платёжных клиринговых позициях;
- информации, необходимой для удостоверения клиентами права распоряжения денежными средствами, в том числе:
    - вся информация, считываемая с магнитной полосы, платежной карты, микропроцессора или другого носителя;
    - проверочный номер карты, используемый для подтверждения операций;
    - ПИН или зашифрованный ПИН-блок;
- ключевой информации средств криптографической защиты информации, используемых при осуществлении переводов денежных средств;
- информации о конфигурации, определяющей параметры работы технических средств защиты информации;
- информации об остатках электронных денежных средств;

- информации о совершенных переводах денежных средств, в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников, а также в извещениях (подтверждениях), касающихся исполнения распоряжений Участников;
- информации, содержащейся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов операторов по переводу денежных средств, распоряжениях Участников, распоряжениях Платежного клирингового центра;
- информации ограниченного доступа, в том числе персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством РФ, обрабатываемой при осуществлении переводов денежных средств.

Требования по защите информации применяются к Оператору платежной системы в части той информации, которая находится в его распоряжении.

Участники и Операторы услуг платежной инфраструктуры обязаны использовать средства криптографической защиты данных в случаях, предусмотренных федеральными законами и иными нормативно-правовыми актами РФ, требованиями Банка России, Правилами и международными стандартами информационной безопасности в соответствии с Правилами.

Соблюдение требований защиты информации осуществляется Оператором платежной системы в порядке, установленном Стандартом Безопасности Данных Индустрии Платёжных Карт (PCI DSS) или другими стандартами защиты информации, признаваемыми PCI DSS. Оператор платёжной системы информирует Участников о выявленных в Платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в соответствии с Правилами.

Оператор платежной системы, Операторы услуг платежной инфраструктуры и Участники обязаны принимать меры, направленные на внесение необходимых изменений в процедуры и процессы обеспечения безопасности и защиты информации в связи с:

- изменением требований к безопасности и защите информации, установленных Правилами;
- изменением требований законодательства РФ и требований Банка России.

### 4.2. Функции Операционного центра по обеспечению безопасности и защиты информации

Операционный центр выполняет следующие основные функции по обеспечению безопасности и защиты информации Платежной системы:

- разрабатывает стратегию обеспечения безопасности и защиты информации и доводит ее до Участников;
- обеспечивает целостность, подлинность и конфиденциальность информации обо всех Участниках на всех этапах её обработки и передачи;
- выполняет процедуры безопасного распределения криптографических ключей, применяемых при обработке и передаче информации между Участниками, Операторами услуг платежной инфраструктуры и Оператором платежной системы;
- следит за обменом авторизационными и клиринговыми сообщениями с целью раннего обнаружения угроз безопасности Платежной системы и отдельных Участников;
- сообщает Участникам об угрозах их безопасности и безопасности Платежной системы и предлагает меры по предотвращению этих угроз.

## 4.3. Проверка и оценка

### 4.3.1. Проверка требований защиты информации Оператором платежной системы

Оператор платежной системы проводит проверку соблюдения Участниками требований к защите информации не реже одного раза в два года. Проверка производится специалистами Оператора платежной системы или независимой организацией. Проверка проводится на соответствие требованиям Положения 382-П, а также в соответствии с требованиями настоящих Правил.

Участник может быть освобожден от очередной проверки по усмотрению Оператора платежной системы, если по результатам последней оценки, проведенной согласно Положению 382-П Участником самостоятельно или сторонней организацией на договорной основе, было получено подтверждение о соответствии стандарту PCI DSS или получен итоговый показатель оценки обеспечения защиты информации не ниже 0,70.

### 4.3.2. Внутренняя оценка защиты информации Участниками

Участники, осуществляющие обработку Карт UnionPay, а также передачу и обработку информации об операциях по Картам UnionPay обязаны ежегодно проводить внутреннюю проверку защиты информации. Участник обязан привлечь для проведения проверки независимую организацию в следующих случаях:

- Годовой объём операций ТСП (как обычных, так и онлайновых ТСП, как отдельно, так и с Операторами услуг платёжной инфраструктуры) с Картами UnionPay достигает следующих уровней.

| | Число операций с Картами UnionPay в год |
|---|---|
| Обычные ТСП | >= 1,5 млн. операций |
| Онлайновые ТСП | >= 0,5 млн. операций |

- У Участника за последний год произошел инцидент с несанкционированным доступом к информации, который был классифицирован как Инцидент Второго Уровня или более высокого уровня (в соответствии с определением в пункте 4.10.3 Правил).
- Участник получил от Оператора платежной системы требование о проведении независимой проверки соответствия требованиям защиты информации.

Оператор платежной системы поощряет стремление Участников периодически проводить независимые проверки соответствия требованиям защиты информации и при отсутствии описанных выше критериев.

### 4.3.3. Порядок проведения проверки или оценки

До конца марта каждого года Оператор платежной системы формирует перечень Участников, подлежащих проверке независимой организацией, на основе объёма проведенных операций по Картам UnionPay. Другие Участники, не включённые в перечень, должны провести внутреннюю оценку с использованием специальной анкеты.

Заполнение анкет внутренней оценки непрямыми Участниками должно проходить под контролем прямых Участников. Участники обязаны устранить недостатки, выявленные по результатам внутренней оценки и к концу года и представить Оператору платежной системы соответствующий отчёт. Оператор платежной системы проверяет результаты самооценки и устранение выявленных недостатков на выборочной основе.

Оператор платежной системы направляет Участникам, которые должны проводить независимую оценку в обязательном порядке, уведомление о проведении независимой оценки соответствия. Участники обязаны завершить независимую оценку соответствия в течение 90 рабочих дней с даты такого уведомления.

Участники должны начать независимую оценку соответствия в течение 20 рабочих дней после получения уведомления и представить Оператору платежной системы отчёт о начале проверки, содержащий следующую информацию:

- контактные данные сотрудников, отвечающих за проведение оценки соответствия;
- разработанный план оценки соответствия;
- результаты проведенный внутренней оценки с использованием специальной анкеты;
- выбранную независимую организацию для проведения оценки соответствия.

Расходы, связанные с проведением оценки, должны покрываться самим Участником.

В течение 15 рабочих дней после завершения независимой оценки, Участник должен утвердить отчёта по результатам оценки и представить Оператору платежной системы следующие материалы.

- отчёт по результатам оценки соответствия в сфере защиты информации о счетах по Картам UnionPay;
- план повышения эффективности работы по обеспечению защиты информации о счетах по Картам UnionPay (по мере необходимости);
- форма для комментариев по вопросам соответствия в сфере защиты информации о счетах по Картам UnionPay.

Оператор платежной системы оценивает материалы, представленные Участниками, в течение 15 рабочих дней с даты их получения.

Участники, которые не сумели обеспечить соответствие действующим требованиям защиты информации, обязаны устранить выявленные недостатки в течение 3 месяцев и представить Оператору платежной системы отчёты по результатам этой работы.

Оператор платежной системы оценивает отчёты об устранении недостатков и принимает решение о необходимости проведения повторной оценки.

Если оцениваемый Участник не проходит повторную оценку, Оператор платежной системы вправе применить к такому Участнику санкции, предусмотренные Правилами.

## 4.4. Требования в отношении сторонних провайдеров услуг и ТСП

### 4.4.1. Обязательства Участников

#### 4.4.1.1. Управление сторонними провайдерами услуг и ТСП

Участники обязаны регулярно (не реже одного раза в год) проводить проверки и аудиты своих сторонних провайдеров услуг и ТСП с целью удостовериться в том, что требования, применимые к сторонним провайдерам услуг и ТСП, соблюдаются надлежащим образом. Если сторонние провайдеры услуг и ТСП не выполняют правила безопасности, необходимо принять соответствующие меры, обеспечивающие соблюдение всех применимых требований.

Участники принимают на себя всю полноту ответственности за безопасность информации

о счетах и данных по операциям своих сторонних провайдеров услуг и ТСП. В то же время Участники обязаны периодически представлять в адрес Оператора платежной системы отчёты о применяемых ими методах и способах обеспечения безопасности информации о счетах и данных по операциям.

#### 4.4.1.2. Требования при подписании соглашений со сторонними провайдерами услуг и ТСП

Соглашения определяют ответственность сторонних провайдеров услуг и ТСП за обеспечение безопасности информации о счетах и данных по операциям. Для всех организаций, которые взаимодействуют с Участниками и имеют доступ к информации о счетах и данным по операциям (в том числе для сторонних провайдеров услуг и ТСП), подписанные соглашения, договоры и приложения к ним должны содержать:

- положение о запрете на предоставление информации о счетах и данных по операциям третьим лицам без прямого согласия в письменном виде;
- требование о том, чтобы соответствующие организации взяли на себя все убытки, вызванные искажением, раскрытием или повреждением информации о счетах и данных по операциям по причине несоответствия процедур управления информацией о счетах и данными по операциям установленным требованиям;
- указание на наличие у Участника права аннулировать или расторгнуть соглашение со сторонним провайдером услуг в случае его неспособности обеспечить соответствие требованиям Правил и иных требований UnionPay об управлении информацией о счетах и данными по операциям;
- положение о безоговорочном содействии, которое должно быть оказано в процессе проверки уровня безопасности соответствующей информации о счетах и соответствующих данных по операциям, проводимой Участником или Оператором платежной системы.

### 4.4.2. Требования к ТСП и сторонним провайдерам услуг

Запрещено предоставлять информацию о счетах и данные по операциям какой бы то ни было третьей стороне, которая не является Эквайрером или организацией, назначенной Эквайрером.

За исключением сторонних провайдеров услуг, специализирующихся на аутсорсинге систем эмиссии карт, другие организации вправе хранить только самую основную информацию о счетах и самые основные данные по операциям, требующиеся для клиринга операций, причём хранение информации, содержащейся на магнитной полосе, кодов проверки подлинности карт и индивидуальных паролей запрещается.

Информация о счетах и данные по операциям могут использоваться только для сопровождения операций по Картам UnionPay и не применяться в каких бы то ни было других целях или передаваться любым неуполномоченным лицам или организациям.

Ни один сторонний провайдер услуг не вправе модифицировать и обслуживать оборудование, содержащее информацию о счетах и данные по операциям, без разрешения Эквайрера или Оператора платежной системы.

## 4.5. Управление персоналом и организациями

Каждый Участник обеспечивает сбор информации о системе управления безопасностью, правилах и процедурах расследования в отношении безопасности информации о счетах и данных

по операциям, а также чётко определяет права и обязанности своих сотрудников в сфере обеспечения защиты информации.

Все сотрудники Участников, имеющие доступ к информации о счетах и данным по операциям, обязаны подписать соглашения о неразглашении конфиденциальной информации.

## 4.6. Защита, использование и уничтожение данных

### 4.6.1. Защита данных

Вся информация о счетах и все данные по операциям должны быть надёжно защищены. Информация о счетах и данные по операциям включают в себя информацию, которая хранится в компьютерных системах различных типов, POS-терминалах, банкоматах и других терминалов, данные, которые передаются по сети и отображаются на экране компьютера, а также данные, которые распечатываются POS-терминалами и банкоматами.

Ответственность за хранение информации о счетах и данных по операциям, которые находятся на резервных носителях информации, таких как кассеты и компакт-диски, возлагается на конкретное лицо. Данные должны храниться в помещении или сейфе, оборудованном системой защиты от несанкционированного доступа.

### 4.6.2. Использование данных

Информация о счетах и данные по операциям Участников не могут быть предоставлены какому бы то ни было третьему лицу без письменного согласия Участника.

Подлинная информация о счетах и подлинные данные по операциям не должны использоваться при разработке программного обеспечения и проведении его испытания методом моделирования. В особых случаях, когда для разработки и тестирования программного обеспечения требуются подлинная информация о счетах и подлинные данные по операциям, для их использования необходимо наличие письменного согласия Участника и подписанного соглашение о неразглашении конфиденциальной информации. Информация и данные должны храниться уполномоченным лицом и должны быть незамедлительно уничтожены по завершении разработки и тестирования.

### 4.6.3. Уничтожение данных

Участники вправе определять срок хранения информации о счетах и данных по операциям в соответствии с законодательством РФ. По истечении установленного срока хранения информация о счетах и данные по операциям подлежат уничтожению.

## 4.7. Управление системой

Информация о счетах и данные по операциям должны храниться и передаваться в системе с применением защитных мер безопасности, включая обеспечение безопасности сети, установку и обновление межсетевого экрана, и реализацию других мер, включая, помимо прочего, установку антивирусного программного обеспечения.

Если внутренняя сеть подсоединена к внешней сети, необходимо осуществлять сетевой мониторинг в целях своевременного выявления попыток несанкционированного проникновению во внутреннюю сеть.

Если пользователи получают доступ к информации о счетах и данным по операциям через открытые сети, они должны быть предупреждены о том, что «при выходе на общедоступные интернет-сайты и получении доступа к информации о счетах через такие сайты существует вероятность раскрытия данных по операциям».

Авторские права на программное обеспечение, его исходные коды и версии должны пройти тщательную проверку и регистрацию. Необходимо обновлять программное обеспечение операционных систем и своевременно устанавливать пакеты обновлений безопасности программного обеспечения.

Параметры безопасности системы должны регулярно проверяться, причём такие проверки должны включать в себя тестирование на уязвимость, тестирование антивирусов и тестирование эффективности межсетевых экранов.

Данные, передаваемые из внутренней сети во внешнюю или наоборот, должны проходить через межсетевой экран, который должен скрывать защищаемую им сетевую структуру и отправлять предупреждения в случае возникновения нештатных ситуаций.

Настройки по умолчанию, предоставляемые поставщиками системного аппаратного или программного обеспечения, такие как пароли доступа к оборудованию или системам, не могут использоваться в качестве контрольных параметров безопасности системы.

## 4.8. Управление инцидентами с неправомерным доступом к информации

Необходимо установить программы аварийного управления на случай нарушения безопасности информации о счетах и данных по операциям с целью обеспечить своевременное и эффективное управление любыми инцидентами.

При возникновении случаев нарушения безопасности, включая искажение, раскрытие, уничтожение и изменение информации о счетах и данных по операциям, необходимо незамедлительно провести расследование и обеспечить управление инцидентом с направлением напрямую или через Оператора платежной системы соответствующего уведомления в адрес всех заинтересованных организаций с целью принятия мер, направленных на предотвращение дальнейших потерь.

Участники должны сообщать о нарушениях безопасности, связанных с информацией о счетах и данными по операциям, через систему информирования о рисках на сайте Оператора платежной системы в сети Интернет www.unionpayintl.com. ТСП и сторонние провайдеры услуг могут представлять отчёты через соответствующих Участников.

## 4.9. Требование о применении тройного стандарта шифрования данных (СШД)

В Платежной системе действуют следующие требования относительно применения тройного стандарта шифрования данных:

- при получении доступа к Платежной системе Участники должны поддерживать тройной стандарт шифрования данных;
- всё оборудование, обрабатывающее ПИН-коды, включая банкоматы, POS-терминалы, терминалы самообслуживания и т.д., должно поддерживать тройной стандарт шифрования данных.

## 4.10. Возмещение ущерба и штрафные санкции

### 4.10.1. Несоблюдение применимых требований

Оператор платежной системы вправе начислить и наложить на виновного Участника или Оператора услуг платежной инфраструктуры штрафные санкции в следующих случаях:

- Причинение ущерба другим Участникам, Операторам услуг платежной инфраструктуры или Оператору платежной системы в силу раскрытия конфиденциальной информации. В данном случае речь идёт об ущербе, который причинён виновной стороной другим Участникам, Операторам услуг платежной инфраструктуры или Оператору платежной системы вследствие того, что виновная сторона допустила неправомерное раскрытие конфиденциальной информации, не направила своевременное уведомление о раскрытии информации или не оказала содействия в проведении расследования в отношении раскрытия информации;

- Несоблюдение требований обеспечения безопасности и защиты информации. В данном случае речь идёт о ситуациях, когда в ходе расследования в сфере безопасности и защиты информации было установлено, что виновная сторона не соблюдает требования обеспечения безопасности и защиты информации, и такое несоблюдение продолжается в течение 12 месяцев после завершения расследования.

### 4.10.2. Сторона, виновная в раскрытии информации

Виновной стороной признается организация, причинившая ущерб Участнику, Оператору услуг платежной инфраструктуры или Оператору платежной системы вследствие несоблюдения требований безопасности и защиты информации или раскрытия информации.

Участник или Оператор услуг платежной инфраструктуры признаётся виновной стороной, если он причинил ущерб другим Участникам, Операторам услуг платежной инфраструктуры или Оператору платежной системы вследствие несоблюдения требований безопасности и защиты информации или раскрытия информации.

Эквайрер признаётся виновной стороной, если его ТСП причинили ущерб другим Участникам, Операторам услуг платежной инфраструктуры или Оператору платежной системы вследствие несоблюдения требований безопасности и защиты информации или раскрытия информации.

Участник или Оператор услуг платежной инфраструктуры признаётся виновной стороной, если привлечённый им на договорной основе сторонний провайдер услуг причинил ущерб другим Участникам, Операторам услуг платежной инфраструктуры или Оператору платежной системы вследствие несоблюдения требований безопасности и защиты информации или раскрытия информации.

### 4.10.3. Классификация инцидентов раскрытия информации

В случае возникновения инцидента раскрытия информации, сообщение о котором представлено двумя или более Участниками, или Операторами услуг платежной инфраструктуры, или сведения о котором получены из других источников, в том числе от правоохранительных или регулятивных органов, Оператор платежной системы относит такой инцидент к одному из следующих четырёх (4) уровней в зависимости от количества счетов, информация о которых была раскрыта, или суммы убытков:

- **Инцидент Первого Уровня**

  При выполнении любого из следующих условий инцидент квалифицируется как Инцидент Первого Уровня:

  - раскрыта информация о более чем 1 000 карточных счетов Карт UnionPay;
  - сумма убытков превышает эквивалент 5 000 000 долларов США.

- **Инцидент Второго Уровня**

  При выполнении любого из следующих условий инцидент квалифицируется как Инцидент Второго Уровня:

  - раскрыта информация о более чем 600, но менее чем 999 (включительно) карточных счетах Карт UnionPay;

- сумма убытков находится в диапазоне от эквивалента 1 000 000 долларов США до эквивалента 5 000 000 долларов США.

➢ **Инцидент Третьего Уровня**

При выполнении любого из следующих условий инцидент квалифицируется как Инцидент Третьего Уровня:

- раскрыта информация о более чем 200, но менее чем 599 (включительно) карточных счетах Карт UnionPay;
- сумма убытков находится в диапазоне от эквивалента 300 000 долларов США до эквивалента 1 000 000 долларов США.

➢ **Инцидент Четвёртого Уровня**

При выполнении любого из следующих условий инцидент квалифицируется как Инцидент Четвёртого Уровня:

- раскрыта информация о менее чем 200 карточных счетах Карт UnionPay;
- сумма убытков составляет менее эквивалента 300 000 долларов США.

Если инцидент относится к разным уровням по количеству счетов, информация о которых была раскрыта, и по сумме убытков, его следует отнести к более высокому из этих уровней (при этом самым высоким является первый уровень).

### 4.10.4. Штрафные санкции

#### 4.10.4.1. Штрафные санкции за раскрытие информации

Следующие штрафные санкции начисляются и налагаются Оператором платежной системы по его усмотрению на сторону, виновную в раскрытии информации, в зависимости от классификации инцидента:

➢ **Уведомление**

Оператор платежной системы направляет в адрес всех Участников и Операторов услуг платежной инфраструктуры уведомление об инциденте с указанием виновной стороны.

➢ **Расследование и обучение**

Виновная сторона обязана в течение одного месяца предоставить отчёт об устранении нарушения в сфере управления безопасностью и защиты информации, а также дать согласие на проведение Оператором платежной системы соответствующего расследования и обучения сотрудников такой стороны. Виновная сторона несёт все связанные с этим расходы, которые ни при каких обстоятельствах не должны превышать эквивалента 20 000 долларов США.

➢ **Возмещение ущерба**

В случае раскрытия информации виновная сторона обязана выплатить Эмитентам эквивалент 10 долларов США за каждую карту независимо от общей суммы ущерба. Для Инцидента Первого Уровня общая сумма возмещения убытков не превышает эквивалент 400 000 долларов США.

Если выполнены все перечисленные ниже условия, виновная сторона может выплатить

Эмитенту эквивалент 5 долларов США за каждую карту в случае раскрытия информации. При этом для Инцидента Первого Уровня общая сумма возмещения убытков не превышает эквивалента 300 000 долларов США:

- виновная сторона сама выявила инцидент и сообщила о нём Оператору платежной системы;
- письменный отчёт представлен Оператору платежной системы до того, как об инциденте сообщали другие Участники или Операторы услуг платежной инфраструктуры;
- соответствующее решение принято Оператором платежной системы.

Во избежание увеличения масштабов ущерба Эмитенты принимают определённые меры, и в том числе заменяют карты и блокируют платежи по картам, в отношении которых имело место раскрытие информации, в течение 3 месяцев с момента получения уведомления от Оператора платежной системы.

➢ **Штраф**

В случае причинения ущерба другим Участникам, Операторам услуг платежной инфраструктуры или Оператору платежной системы вследствие раскрытия информации о счетах на виновную сторону могут быть наложены следующие штрафы:

- Для Инцидента Первого Уровня сумма штрафа составляет 25% от суммы совокупных убытков, понесённых пострадавшими сторонами, причём общая максимальная сумма не должна превышать эквивалента 500 000 долларов США. Вся сумма штрафа распределяется между пострадавшими сторонами исходя из процентного соотношения понесённых ими убытков.
- Для Инцидента Второго Уровня сумма штрафа составляет 25% от суммы совокупных убытков, понесённых пострадавшими сторонами, причём общая максимальная сумма не должна превышать эквивалента 300 000 долларов США. Вся сумма штрафа распределяется между пострадавшими сторонами исходя из процентного соотношения понесённых ими убытков.
- Для Инцидента Третьего Уровня сумма штрафа составляет 25% от суммы совокупных убытков, понесённых пострадавшими сторонами, причём общая максимальная сумма не должна превышать эквивалента 200 000 долларов США. Вся сумма штрафа распределяется между пострадавшими сторонами исходя из процентного соотношения понесённых ими убытков.
- Для Инцидента Четвёртого Уровня сумма штрафа составляет 25% от суммы совокупных убытков, понесённых пострадавшими сторонами. Вся сумма штрафа распределяется между пострадавшими сторонами исходя из процентного соотношения понесённых ими убытков.

После обнародования Оператора платежной системы уведомления о Картах UnionPay, в отношении которых в результате инцидента имело место раскрытие информации, Эмитенты не вправе требовать компенсации убытков за мошенническое использование таких карт в течение 3 месяцев после такого уведомления.

#### 4.10.4.2. Дополнительные штрафные санкции за повторное раскрытие информации

Если виновная сторона допустила ещё повторный инцидент раскрытия информации в

течение 1 года с момента предыдущего инцидента, помимо штрафных санкций, установленных Оператором платежной системы в соответствии с пунктом 4.10.4.1 Правил, на неё налагается дополнительный штраф в размере эквивалента 100 000 долларов. США.

Вся сумма дополнительного штрафа распределяется между пострадавшими сторонами исходя из процентного соотношения понесённых ими убытков.

#### 4.10.4.3. Штрафные санкции за несоблюдение требований безопасности и защиты информации

Следующие штрафные санкции начисляются и налагаются на сторону, виновную в несоблюдении требований безопасности и защиты информации:

- Если в ходе расследования в сфере безопасности и защиты информации установлено, что Участник или Оператор услуг платежной инфраструктуры не соблюдает или не выполняет требования безопасности, такой Участник или Оператор услуг платежной инфраструктуры обязан представить план устранения нарушений и дать согласие на проведение повторного расследования в соответствии с письменным уведомлением Оператора платежной системы. Участник или Оператор услуг платежной инфраструктуры несёт связанные с этим расходы, включая расходы на проезд и проживание, а также другие расходы, непосредственно связанные с расследованием, общая сумма которых ни при каких обстоятельствах не должна превышать эквивалент 20 000 долларов США.
- Если в ходе повторного расследования установлено, что Участник или Оператор услуг платежной инфраструктуры не соблюдает требования безопасности и защиты информации, на такого Участника или Оператора услуг платежной инфраструктуры налагается штраф в размере эквивалента 50 000 долларов США. Сумма такого штрафа направляется Оператором платёжной системы на проведения расследования и обучения в сфере управления информацией о счетах.
- Если Участник или Оператор услуг платежной инфраструктуры отказывается уплатить штраф или принять меры по устранению нарушений и продолжает делать это после завершения судебного разбирательства, Оператор платежной системы вправе прекратить участие такого Участника в Платежной системе или расторгнуть соглашение с таким Оператором услуг платежной инфраструктуры.

#### 4.10.4.4. Определение виновной стороны и инициирование штрафных санкций

В случае наступления описанных выше событий, Оператор платежной системы инициирует процедуру принятия жалоб, проведения расследований, сбора доказательств, выявления фактов и осуществления других необходимых действий.

#### 4.10.4.5. Освобождение от штрафных санкций

Виновная сторона, несущая ответственность за любой инцидент раскрытия информации, может быть освобождена от штрафных санкций, если она выполняла требования безопасности и защиты информации в соответствии с Правилами.

# Глава 5. Система управления рисками

## 5.1. Модель управления рисками

Согласно статье 28 Закона о НПС, Оператор платёжной системы определил следующую организационную модель управления рисками: распределение функций по оценке и управлению рисками между Оператором платежной системы, Операторами услуг платежной инфраструктуры и Участниками.

НСПК управляет всеми рисками в отношении предоставления операционных услуг и услуг платежного клиринга в Платежной системе, включая взаимодействие с Банком России.

Банк России управляет рисками в отношении предоставления расчетных услуг в Платежной системе, включая взаимодействие с НСПК.

Оператор платёжной системы определяет собственную структуру управления рисками и функциональные обязанности лиц, ответственных за управление рисками (либо соответствующих структурных подразделений).

Участники и Операторы услуг платёжной инфраструктуры самостоятельно определяют в рамках своей деятельности в качестве Субъекта платежной системы собственную структуру управления рисками и функциональные обязанности лиц, ответственных за управление рисками, либо соответствующих структурных подразделений, принимая во внимание требования законодательства РФ, требования Банка России и рекомендаций, изложенных в Правилах.

Правила содержат общие принципы управления рисками. Для организации деятельности по управления рисками Оператор платежной системы разрабатывает и утверждает внутренние документы в области управления рисками. Внутренние документы могут детализировать принципы управления рисками, а также содержать дополнительные мероприятия и способы управления рисками. Внутренним документом, содержащим положения принципов управления рисками, а также дополнительные мероприятия и способы управления рисками, является положение по управлению рисками и обеспечению БФПС.

Положения настоящей главы 5 «*Система управления рисками*» не распространяются на Банк России при выполнении им функций расчетного центра и центрального платежного контрагента. Оператор платежной системы не несет ответственность за риск-менеджмент, его организацию, соблюдение требований риск-менеджмента Банком России и НСПК при выполнении ими расчетных, операционных и платежных клиринговых функций.

## 5.2. Задачи и основные принципы управления рисками в платежной системе

В задачи Участников по обеспечению БПФС входит реализация комплекса мероприятий и способов управления рисками, направленных на выполнение требований, соответствие Правилам, в частности соблюдение критериев вступления и работы в Платежной системе для прямых и косвенных Участников соответственно.

Основными принципами управления рисками в Платежной системе являются:

- Непрерывность - осуществление на постоянной основе процессов управления рисками в Платежной системе;
- Обучение – обеспечение прохождения работниками Оператора платежной системы, вовлеченными в процесс управления рисками в Платежной системе, обучения современным стандартам и лучшим практикам, имеющих значения для обеспечения БФПС;

- Ответственность – установление ответственности за неисполнение порядка обеспечения в Платежной системе БФПС;
- Разграничение полномочий и самостоятельность Субъектов платежной системы в рамках управления рисками в Платежной системе.

Система управления рисками каждого Субъекта платежной системы должна рассматривать его деятельность в целом, в том числе, деятельность, не связанную с участием в Платежной системе, если такая деятельность может стать источником риска, влияющего на способность Субъекта платежной системы выполнять требования Правил или соответствовать критериям участия в ней.

Субъекты платежной системы должны самостоятельно и эффективно управлять рисками финансовых и иных операций, если они могут привести, в том числе:

- к недостаточности средств для выполнения обязательств в рамках Платежной системы (банкротство и пр.);
- ограничению со стороны регуляторов на осуществление основного вида деятельности (отзыв банковской лицензии и пр.);
- решениям органов исполнительной или судебной власти, приводящих к различным ограничениям на взаимодействие с Оператором платежной системы или другими Субъектами платежной системы (решение суда об аресте счетов, и пр.).

### 5.3. Организационная структура управления рисками

Функции по управлению рисками в Платежной системе выполняются следующими структурными подразделениями и сотрудниками Оператора платёжной системы в соответствии с их полномочиями:

- Генеральным директором Оператора платежной системы;
- Заместителем генерального директора;
- другими подразделениями и сотрудниками Оператора платежной системы в рамках их должностных обязанностей.

Информация о рисках регулярно доводится до сведения Генерального директора Оператора платежной системы лицами и подразделениями Оператора платежной системы в соответствии с их обязанностями в виде отчетов. Состав и порядок предоставления информации определяется в положениях, приказах, должностных инструкциях, а также в соответствующих внутренних документах Оператора платежной системы и включает в себя, помимо прочего, отчеты о реализации управления рисками в соответствии с разделом 5.8 Правил. Соответствующие отчеты предоставляются для рассмотрения Генеральному директору каждые три месяца.

### 5.4. Функциональные обязанности по управлению рисками

Структурные подразделения и сотрудники, ответственные за управление рисками в Платёжной системе, выполняют следующие функциональные обязанности в части рисков в Платежной системе, за исключением рисков в части оказания расчетных, платежных клиринговых и операционных услуг:

- регулярный контроль за уровнем рисков Платёжной системы;
- реагирование на изменение уровня рисков Платёжной системы;
- контроль за соблюдением Правил Участниками и Операторами услуг платёжной инфраструктуры;

- внесение изменений в Правила в целях совершенствования системы управления рисками Платёжной системы;
- регулярная оценка уровня риска по каждому выявленному виду рисков;
- исполнение иных обязанностей в целях управления рисками в Платёжной системе.

Распределение обязанностей по управлению рисками между подразделениями и сотрудниками Оператора платёжной системы устанавливается Оператором платёжной системы во внутренних положениях, приказах, должностных инструкциях и иных внутренних документах Оператора платёжной системы.

## 5.5. Управление рисками Операторами услуг платежной инфраструктуры и Участниками

### 5.5.1. Создание внутреннего механизма управления рисками

Участники обязаны назначить структурное подразделение и сотрудников, ответственных за управление рисками, связанными с проведением операций по Картам UnionPay. Такое управление рисками включает в себя, помимо прочего, следующие аспекты:

- разработка и реализация внутренних правил и принципов управления рисками;
- анализ и усовершенствование внутреннего аудита процесса реализации системы управления рисками;
- обеспечение безопасности систем и оборудования обработки Карт UnionPay;
- обеспечение безопасности перевода денежных средств, защиты информации о счетах и данных по операциям;
- создание системы контроля за проведением операций;
- расследование и урегулирование событий наступления рисков.

### 5.5.2. Контактные данные сотрудников, ответственных за управление рисками

Каждый Оператор услуг платежной инфраструктуры (если применимо) и Участник обязан предоставить текущий перечень и контактные данные сотрудников и внутренних подразделений, ответственных за осуществление следующих действий:

- проверка потенциальных ТСП;
- создание и контроль деятельности систем раннего выявления мошеннических операций, проводимых с использованием счетов Держателей карт и ТСП;
- расследование всех случаев мошенничества с использованием Карт UnionPay;
- проведение расследований по запросам других Операторов услуг платежной инфраструктуры или Участников;
- взаимодействие с правоохранительными органами;
- проведение программ по обучению Держателей карт и сотрудников ТСП;
- поддержание контактов с сотрудниками Оператора платежной системы,
- ответственными за управление рисками;
- информирование Оператора платежной системы обо всех подтверждённых мошеннических операциях.

Применение положений настоящего раздела 5.5 «*Управление рисками Операторами услуг платежной инфраструктуры и Участниками*» в отношении Банка России при выполнении им функций Расчетного центра и Центрального платежного клирингового контрагента и НСПК при выполнении им функций Операционного центра и Платежного клирингового центра регулируется законодательством и соответствующими договорами между Оператором платежной системы и соответствующих Операторов услуг платежной инфраструктуры.

Оператор платежной системы не несет ответственность за риск-менеджмент, его организацию, соблюдение требований риск-менеджмента Банком России и НСПК при выполнении ими расчетных, операционных и платежных клиринговых функций.

### 5.6. Противодействие легализации (отмыванию) доходов, полученных преступным путём, и финансированию терроризма

Оператор платежной системы, Операторы услуг платежной инфраструктуры и Участники должны обеспечить соответствие всех проводимых ими операций и всех осуществляемых ими видов деятельности требованиям Федерального закона от 07 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и иных нормативно-правовых актов РФ о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

Контроль за соблюдением банковским платежным агентом условий его привлечения, а также законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, осуществляется непосредственно самим Эквайрером, заключившим с банковским платежным агентом соответствующий договор.

Контроль за аналогичной деятельностью банковского платежного субагента осуществляется банковским платежным агентом, привлекшим такого банковского платежного субагента в соответствии с действующим законодательством РФ и соответствующим договором между банковским платежным агентом и Эквайрером.

### 5.7. Виды рисков в Платежной системе

В рамках системы управления рисками в Платежной системе выделяются следующие виды рисков, подлежащие оценке и мониторингу:

- Правовой риск;
- Операционный риск;
- Кредитный риск;
- Риск ликвидности;
- Общий коммерческий риск.

### 5.8. Способы управления рисками в Платежной системе

Способы управления рисками определяются Оператором платежной системы с учетом особенностей организации Платежной системы, модели управления рисками, процедур платежного клиринга и расчетов по итогам клиринга, количества переводов денежных средств и их сумм, времени окончательного расчета и подразделяются на общие (применяются для управления различными видами рисков) и специальные (применяются для управления одним видом рисков).

Система управления рисками предусматривает следующие общие способы управления рисками:

- наблюдение за осуществлением расчетов и случаями несвоевременного осуществления расчетов Расчетным центром и исполнения обязательств Участниками;
- регулярный анализ соответствующей отчетности в целях выявления рисков Субъектов платежной системы;
- анализ показателей БФПС;
- установление предельных размеров обязательств (авторизационных лимитов) Участников с учетом соответствующего уровня риска;
- обеспечение возможности предоставления кредита;
- использование безотзывной банковской гарантии или аккредитива;
- использование обеспечения в виде денежных средств, размещаемых на отдельных банковских счетах.

Система управления рисками предусматривает следующие специальные способы управления рисками:

- Для Правового риска:
  - стандартизация Субъектами платежной системы порядка заключения и исполнения сделок (порядки, процедуры, технологии осуществления операций и сделок, заключения договоров);
  - установление Субъектами платежной системы внутреннего порядка согласования заключаемых договоров и их исполнения, особенно в части нестандартных сделок;
  - анализ влияния факторов Правового риска на показатели деятельности Субъекта платежной системы;
  - осуществление Субъектами платежной системы на постоянной основе мониторинга изменений законодательства РФ и, если применимо, стран местонахождения их зарубежных филиалов, дочерних и зависимых организаций;
  - подчинение юридической службы Субъекта платежной системы единоличному исполнительному органу либо построение эффективной коммуникации с внешним юридическим консультантом;
  - оптимизация нагрузки на сотрудников юридической службы, обеспечивающая постоянное повышение квалификации;

- обеспечение доступа максимального количества служащих к актуальной информации по законодательству;
- стимулирование служащих в зависимости от влияния их деятельности на уровень правового риска.

- Для Операционного риска:
  - регламентирование порядка выполнения основных процессов в Правилах и внутренних документах Оператора платежной системы;
  - регламентирование порядка совершения всех основных операций в рамках внутренних нормативно-методологических документов;
  - учет и документирование совершаемых операций, регулярные выверки расчетных документов по операциям;
  - применение принципов разделения и ограничения функций, полномочий и ответственности сотрудников, использование механизмов двойного контроля, принятия коллегиальных решений, установления ограничений на сроки и объемы операций;
  - реализация процедур административного и финансового внутреннего контроля (предварительного, текущего и последующего) за организацией бизнес-процессов, деятельностью Участников и совершением операций отдельными сотрудниками, соблюдением сотрудниками требований действующего законодательства РФ и внутренних нормативных документов, контроль за соблюдением установленных лимитов по проводимым операциям, порядка доступа к информации;
  - автоматизация проведения операций, использование информационных систем;
  - обеспечение информационной безопасности, контроль над доступом к информации, применение многоуровневой защиты информации с использованием сертифицированных средств защиты информации, а также с аттестацией объектов информатизации Платежной системы по требованиям информационной безопасности;
  - создание необходимых организационных и технических условий для обеспечения БФПС при совершении операций (на случай аварий, пожаров, терактов и других непредвиденных ситуаций);
  - снижение рисков, связанных с персоналом, путем установления критериев по его отбору и проведения предварительной проверки, реализации мероприятий по подготовке и обучению персонала, повышению его квалификации.

- Для Кредитного риска и Риска ликвидности:

- выполнение Участниками требований по финансовому обеспечению расчетов в Платежной системе;
- выполнение Операционным центром мониторинга объемов операций, оперативный контроль резкого роста объемов операций того или иного Участника;
- проведение анализа и оценка соотношения активов и пассивов по степени ликвидности, т.е. активы и пассивы распределяются по соответствующим группам по степени убывания ликвидности и с учетом их срока и качества;
- контроль соблюдения Операционным центром и Расчетным центром процедур выполнения Участниками требований по финансовому обеспечению расчетов в рамках Платежной системы;
- контроль финансовой устойчивости Участников в соответствии с Правилами и выполнения Операционным центром мониторинга объемов межбанковских операций, оперативный контроль резкого роста объемов межбанковских операций того или иного Участника;
- соблюдение Участниками правил о своевременном представлении форм финансовой отчетности, предусмотренных Правилами, и выполнение Участниками требований по финансовому обеспечению расчетов в Платежной системе.

- Для Общего коммерческого риска:
  - поддержание системы управления и контроля для выявления, мониторинга и управления общими бизнес-рисками, включая потери от невыполнения бизнес-стратегии, отрицательных денежных потоков или неожиданных и чрезмерно больших операционных расходов;
  - сохранение ликвидных чистых активов Оператора платежной системы, финансируемых за счет собственных средств, в целях продолжения осуществления операций и услуг, а также покрытия текущих и прогнозируемых операционных расходов в рамках ряда сценариев, в том числе в неблагоприятных рыночных условиях;
  - обеспечить строгое соблюдение правил инвестирования и процедур мониторинга иных рисков.

**5.9. Основные этапы управления рисками**

1. Идентификация риска - выявление риска, определение причин и предпосылок, которые могут повлиять на БФПС.
2. Анализ и оценка риска - анализ информации, полученной в результате идентификации риска, определение вероятности наступления рисковых событий, влияющих на БФПС.
3. Разработка и проведение мероприятий по ограничению, снижению, предупреждению риска.

4. Мониторинг уровня риска - выявление событий, способствующих изменению степени подверженности риску, уровня риска, отслеживание динамики характеризующих уровень риска показателей с целью выявления отклонений и определению тенденций в изменении уровня риска;

## 5.10. Профили рисков

### 5.10.1. Правовой риск

Для целей Правового риска, Риск-событиями являются (1) возникновение финансовых потерь, (2) наложение органами, выполняющими регуляторную функцию, и иными правоприменительными органами санкций в связи с нарушением применимого законодательства, в каждом случае в той мере, насколько это может оказать существенное отрицательное воздействие на БФПС.

Источниками (причинами) Риск-события являются:

- внутренние факторы:
  - несоблюдение Субъектами платежной системы законодательства РФ;
  - несоответствие внутренних документов Субъектов платежной системы законодательству РФ;
  - неэффективная организация правовой работы Субъектами платежной системы, приводящая к правовым ошибкам;
  - нарушение Субъектами платежной системы условий договоров, а также;
  - недостаточная проработка правовых вопросов при разработке и внедрении Субъектами платежной системы новых технологий и условий осуществления деятельности, а также при внедрении различного рода инноваций и технологий.
- внешние факторы:
  - несовершенство нормативно-регуляторной базы, ее подверженность частым изменениям, а также отсутствие единообразия в толковании нормативно-регуляторных норм;
  - нарушение условий договоров Субъектами платежной системы (с позиции Субъекта платежной системы, не нарушавшего договор);
  - применимость положений международного или наднационального законодательства, которые могут вступать в противоречие с нормами российского права (неопределенность касательно применимости таких положений); и
  - наличие положений иностранного законодательства, опосредованная применимость которых к Субъектам платежной системы может быть обоснована иностранным участием в капитале соответствующего Субъекта платежной системы.

Наиболее вероятными случаями наступления указанных Риск-событий являются:

- ошибки при оценке положений нормативных (регуляторных) актов, в том числе применительно к вновь вступающим в силу нормативным актам, а также при внедрении различного рода инноваций и технологий;
- недостаточная проработка условий договоров при выполнении договорной работы;
- запуск инновационных продуктов/технологий без одобрения Оператора платежной системы.

Вероятность реализации в Платежной системе правовых Риск-событий оценивается как низкая. Оценка обусловлена:

- в отношении Оператора платежной системы – наличием эффективного взаимодействия по правовым вопросам с внешним юридическим консультантом;
- в отношении Операторов услуг платежной инфраструктуры – в связи с тем, что Операторами услуг платежной инфраструктуры являются Банк России и АО «НСПК», организация должного юридического сопровождения их деятельности презюмируется;
- в отношении Участников – в силу рода деятельности Участников (кредитные организации) юридическая работа которых налажена должным образом.

Возможными неблагоприятными последствиями Риск-событий являются:

- существенные материальные потери, возникшие у Субъекта(-ов) платежной системы;
- меры воздействия, выражающиеся в приостановлении деятельности либо отзыве лицензии (если применимо) того ил иного Субъекта платежной системы;
- предъявление претензий правового характера к деятельности Участников и Операторов услуг платежной инфраструктуры.

Реализация Правового риска может повлиять на функционирование Субъектов платежной системы вплоть до прекращения / остановки деятельности (отзыва лицензии).

Риск-события в рамках Правового риска являются актуальными для всех Субъектов платежной системы.

### 5.10.2. Операционный риск

Для целей Операционного риска, Риск-событиями являются убытки, возникшие у Субъектов платежной системы в результате причин, описанных ниже.

Источниками (причинами) Риск-события являются:

- случайные или преднамеренные действия физических и (или) юридических лиц, направленные против интересов Субъектов платежной системы или Платежной системы в целом;
- несовершенство организационной структуры Субъектов платежной системы в части распределения полномочий подразделений и сотрудников, порядков и процедур совершения операций в рамках Платежной системы, их документирования и отражения в учете;
- несоблюдение сотрудниками Субъектов платежной системы установленных порядков и процедур, неэффективность внутреннего контроля;
- сбои в функционировании информационных систем и оборудования Субъектов платежной системы;
- неблагоприятные внешние обстоятельства, находящиеся вне контроля Оператора платежной системы и (или) Субъектов платежной системы в целом.

Риск-событие наступает в случае:

- злоупотреблений или противоправных действий, осуществляемых служащими или с участием служащих Субъекта платежной системы (например, хищение, злоупотребление служебным положением, несанкционированное использование информационных систем и

ресурсов);

- противоправных действий сторонних по отношению к Субъекту платежной системы (третьих) лиц (например, подлог и (или) подделка платежных и иных документов, несанкционированное проникновение в информационные системы);
- нарушений Субъектом платежной системы или его служащими трудового законодательства (например, нарушение условий трудового договора, причинение вреда здоровью служащих);
- повреждения или утраты основных средств и других материальных активов (в результате актов терроризма, стихийных бедствий, пожара);
- выхода из строя оборудования и систем (например, сбой (отказ) в работе компьютерных систем, систем связи, поломка оборудования);
- ненадлежащей организации деятельности, ошибок управления и исполнения (например, в результате неадекватной организации внутренних процессов и процедур, отсутствия (несовершенства) системы защиты и (или) порядка доступа к информации, неправильной организации информационных потоков внутри Субъекта платежной системы, невыполнения обязательств перед Субъектом платежной системы поставщиками услуг (исполнителями работ), ошибок при вводе и обработке данных по операциям и сделкам, утери документов и т.п.).

Вероятность реализации в Платежной системе Операционного риска оценивается как средняя. Оценка обусловлена характером деятельности, усложненным прогнозированием и многообразием как факторов, оказывающих влияние на реализацию риска, так и источников его реализации (а именно: внешние факторы, человеческий фактор, технологии, системы, оборудование).

Возможными неблагоприятными последствиями Риск-события являются:

- снижение стоимости активов;
- досрочное списание (выбытие) материальных активов;
- денежные выплаты на основании постановлений (решений) судов, решений органов, уполномоченных в соответствии с законодательством РФ;
- денежные выплаты клиентам и контрагентам, а также служащим соответствующего Субъекта платежной системы в целях компенсации им во внесудебном порядке убытков, понесенных ими по вине такого Субъекта платежной системы;
- затрат на восстановление хозяйственной деятельности и устранение последствий ошибок, аварий, стихийных бедствий и других аналогичных обстоятельств;
- прочие убытки.

Реализация Операционного риска может повлиять на:

- БФПС;
- исправное функционирование информационных систем Субъектов платежной системы, количество незавершенных банковский операций;
- снижение стоимости активов Субъекта платежной системы;
- снижение способности Оператора платежной системы и иных Субъектов платежной системы осуществлять управление Операционным риском и иными рисками;

- увеличение Риска Ликвидности у Участников.

### 5.10.3. Кредитный риск

Для целей Кредитного риска, Риск-событиями являются оказание услуг платежной инфраструктуры, не соответствующих требованиям к оказанию услуг, Платежным клиринговым центром или Расчетным центром вследствие невыполнения Участниками договорных обязательств перед указанными организациями в установленный срок или в будущем.

Источниками (причинами) Риск-события являются:

- Сокращение объема гарантийного обеспечения, предоставленного Участником для покрытия внутридневного кредита, до меньшего объема, чем сумма предоставленного кредита;
- Несвоевременное изменение размера гарантийного обеспечения по требованию Оператора платежной системы.

Риск-событие наступает в случае, если:

- Участник не своевременно выполняет обязательства по формированию гарантийного обеспечения;
- Платежный клиринговый центр или Расчетный центр предоставляет информацию о нарушении Участником договорных обязательств.

Вероятность наступления Риск-события низкая. Оценка обусловлена процедурой формирования гарантийного обеспечения, и низкой вероятностью нарушения Участниками договорных обязательств с Платежным клиринговым центром и Расчетным центром.

Возможными неблагоприятными последствиями Риск-события являются:

- задержки в осуществлении Участниками расчетов и клиринга;
- денежные выплаты на основании постановлений (решений) судов, решений уполномоченных органов;
- прочие убытки.

Реализация Кредитного риска может повлиять на:

- исправное функционирование Субъекта платежной системы;
- увеличение Риска Ликвидности у Участника.

### 5.10.4. Риск ликвидности

Для целей Риска ликвидности, Риск-событиями являются случаи неспособности Участников или других организаций своевременно выполнять свои платежные обязательства в рамках клирингового или расчетного процесса.

Источниками (причинами) Риск-события являются:

- невыполнение обязательств Участником своих денежных обязательств перед иными Участниками;
- Недостаточный объем собственных денежных средств для завершения расчетов.

Риск-событие наступает в случае, если:

- Участник не имеет денежных средств на расчетном счете в Расчетном центре,

необходимых для оплаты своих денежных обязательств;

- Расчетный центр не может перевести денежные средства Участников в связи с кризисом ликвидности.

Вероятность наступления Риск-события средняя. Оценка обусловлена статистикой наступления Риск-событий в прошлом.

Возможными неблагоприятными последствиями Риск-события являются:

- необходимость оплаты задолженности Участника перед другими Участниками Оператором платежной системы на основании отдельного письма – требования от Расчетного центра;
- прочие убытки.

Реализация Риска ликвидности может повлиять на:

- исправное функционирование Субъекта платежной системы;
- увеличение других видов риска.

### 5.10.5 Общий коммерческий риск

Для целей Общего коммерческого риска, Риск-событием является любое потенциальное ухудшение финансового состояния Оператора платежной системы (как коммерческого предприятия) вследствие уменьшения его доходов или увеличения расходов, при котором расходы превышают доходы, приводя к потерям, которые могут быть отнесены на капитал.

Источниками (причинами) Риск-события являются:

- неблагоприятные репутационные эффекты;
- плохая реализация бизнес-стратегии;
- неэффективная реакции на конкуренцию;
- потери по другим видам коммерческой деятельности Оператора платежной системы или ее материнской компании или действия других коммерческих факторов.

Риск-событие наступает в случае, если:

- финансовое состояние Оператора платежной системы непрерывно ухудшается в течении 2 лет;
- внешние рейтинговые агентства присваивают негативный финансовый рейтинг Оператору платежной системы.

Вероятность наступления Риск-события - низкая. Оценка обусловлена финансовой поддержкой основного учредителя Оператора платежной системы.

Возможными неблагоприятными последствиями Риск-события являются:

- выход Участников из Платежной системы;
- увеличение других видов рисков;
- прочие убытки.

Реализация Общего коммерческого риска может повлиять на:

- исправное функционирование Субъектов платежной системы;

- увеличение других видов риска.

## 5.11. Показатели БФПС и порядок обеспечения БФПС

В целях обеспечения БФПС Оператором платежной системы устанавливается порядок осуществления Участниками скоординированной деятельности, направленной на достижение, подтверждение и поддержание приемлемого уровня рисков нарушения БФПС, под которыми понимаются присущие функционированию Платежной системы типичные возможности неоказания, ненадлежащего оказания услуг Участникам вследствие наступления неблагоприятных событий, связанных с внутренними и внешними факторами функционирования Платежной системы.

Порядок обеспечения БФПС включает:

- способы обеспечения БФПС;
- Показатели БФПС;
- методики анализа рисков в Платежной системе, включая профили рисков, систему управления рисками нарушения БФПС;
- иные требования по обеспечению БФПС.

Оператор платежной системы обеспечивает регламентацию порядка обеспечения БФПС и деятельность по его реализации.

Оператор платежной системы определяет Показатели БФПС, методики анализа рисков в Платежной системе в соответствии с требованиями законодательства РФ.

С целью обеспечения БФПС Оператор платежной системы осуществляет:

- сбор, систематизацию, накопление информации о переводах денежных средств;
- недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих учет информации о переводах, платежных позициях Участников и состоянии расчетов (организация бесперебойности электропитания, дублирование каналов связи и вычислительных мощностей, резервное копирование баз данных, защита информационных систем от воздействия вредоносного программного обеспечения);
- устранение нарушений в случае их возникновения;
- анализ причин нарушений функционирования операционных и технологических средств, устройств, информационных систем, выработку и реализацию мер по их устранению;
- обеспечение сохранения функциональных возможностей операционных и технологических средств, устройств, информационных систем при сбоях в их работе (отказоустойчивость), проведение их тестирования в целях выявления
- недостатков функционирования, а в случае выявления указанных недостатков - принятие мер по их устранению;
- обеспечение собственной финансовой устойчивости: ликвидности, экономических нормативов, финансовых показателей;
- поддержание Участниками на банковских счетах остатка денежных средств достаточного для осуществления бесперебойных расчетов с Оператором платежной системы, в том числе установление минимального неснижаемого остатка;

- иные способы с целью обеспечения БФПС.

Оператор платежной системы организует управление рисками нарушения БФПС, включающее:

- установление приемлемого уровня рисков нарушения БФПС;
- анализ рисков нарушения БФПС (выявление факторов риска нарушения БФПС; определение степени и характера влияния указанных факторов на БФПС; оценку достигнутого уровня рисков нарушения БФПС, под которым понимается размер возможного ущерба, причиняемого Участникам, Держателям карт вследствие нарушений надлежащего функционирования Платежной системы, с учетом вероятности возникновения указанных нарушений в течение прогнозируемого периода времени; подтверждение соответствия достигнутого уровня рисков нарушения БФПС установленному приемлемому уровню рисков нарушения БФПС);
- принятие мер, необходимых для достижения или поддержания приемлемого уровня рисков нарушения БФПС;
- выявление текущих изменений достигнутого уровня риска нарушения БФПС (мониторинг рисков нарушения БФПС);
- информационное взаимодействие Участников в целях управления рисками нарушения БФПС.

Оператор с учетом особенностей функционирования Платежной системы определяет:

1. Организационные аспекты взаимодействия Участников при осуществлении деятельности по обеспечению БФПС.
2. Требования к содержанию деятельности по обеспечению БФПС осуществляемой Оператором платежной системы, Операторами услуг платежной инфраструктуры, прямыми и косвенными Участниками.
3. Порядок информационного взаимодействия Субъектов платежной системы и документационного обеспечения их деятельности по обеспечению БФПС.

Применение положений настоящего раздела 5.11 «*Показатели БФПС и порядок обеспечения БФПС*» в отношении Банка России при выполнении им функций Расчетного центра и Центрального платежного клирингового контрагента и НСПК при выполнении им функций Операционного центра и Платежного клирингового центра регулируется законодательством и соответствующими договорами между Оператором платежной системы и Операторами услуг платежной инфраструктуры.

Оператор платежной системы не несет ответственность за риск-менеджмент, его организацию, соблюдение требований риск-менеджмента Банком России и НСПК при выполнении ими расчетных, операционных и платежных клиринговых функций.

**5.11.1. Организационные аспекты взаимодействия Субъектов платежной системы при осуществлении деятельности по обеспечению БФПС**

Организационные аспекты взаимодействия Субъектов платежной системы при осуществлении деятельности по обеспечению БФПС включают:

(1) Организационную модель управления рисками в Платежной системе

В рамках организационной модели управление рисками:

Управлением рисками в Платежной системе осуществляет Оператор платежной

системы, Операторы услуг платежной инфраструктуры и Участники – на постоянной основе.

Основные функциональные обязанности должностных лиц Оператора платежной системы либо соответствующих структурных подразделений Оператора платежной системы, ответственных за управление рисками в Платежной системе, распределены следующим образом:

a) Генеральный директор (на постоянной основе):

- утверждение политики управления рисками;
- распределение полномочий и ответственности по управлению рисками между руководителями подразделений различных уровней, сотрудниками, ответственными за оценку уровня рисков, обеспечение их необходимыми ресурсами, установление порядка взаимодействия и представления отчетности;
- утверждение внутренних документов Оператора платежной системы, регулирующих основные принципы управления рисками Платежной системы;
- создание и функционирование эффективного внутреннего контроля и риск-менеджмента, осуществление контроля за полнотой и периодичностью проверок Платежной системы внутреннего контроля соблюдения основных принципов управления рисками;
- осуществление контроля за полнотой и периодичностью предоставляемых отчетов об оценке уровня рисков;
- оценка эффективности управления рисками;
- контроль функционирования Платежной системы;
- обеспечение контроля за финансовыми операциями.

b) Департамент по управлению рисками

- определение правил и процедур управления рисками, руководство разработкой внутренних документов по управлению рисками (положений, порядков, правил, методик, регламентов и т.п.);
- определение соответствия действий и операций, осуществляемых руководством и служащими Оператора платежной системы, требованиям законодательства РФ, внутренних документов Оператора платежной системы, определяющих проводимую Оператором платежной системы политику, процедуры принятия и реализации решений, организации учета и отчетности, включая внутреннюю информацию о принимаемых решениях, проводимых операциях (заключаемых сделках), результатах анализа финансового положения (в соответствии с планами внутренних проверок);
- инициация внесения изменений в Правила в целях управления рисками в Платежной системе (по мере необходимости);
- вынесение предложений в целях управления рисками на рассмотрение Генерального директора (по мере необходимости);

- контроль за соблюдением процедур по управлению рисками Платежной системы (на постоянной основе);
- участие в разработке внутренних документов Оператора платежной системы с целью проверки соответствия их содержания требованиям законодательства РФ и системы внутреннего контроля (на постоянной основе);
- выявление, измерение и определение приемлемого уровня риска по каждому из видов рисков (по мере необходимости, но не реже 1 раза в год);
- мониторинг рисков (на постоянной основе);
- сбор и обработка информации в рамках системы управления рисками;
- контроль за ведением лимитов (на постоянной основе);
- оперативное информирование Генерального директора о случаях, которые могут повлечь за собой реализацию рисков, возникновении негативных тенденций;
- контроль за наличием у Оператора платежной системы чистых активов в размере не менее 10 (десяти) миллионов рублей.

Система управления рисками Операторами услуг платежной инфраструктуры и Участниками определяется ими самими в соответствии с Правилами и законодательством РФ.

(2) Определение Субъекта платежной системы, осуществляющего координацию деятельности по обеспечению БФПС.

Субъектом платежной системы, осуществляющим координацию деятельности по обеспечению БФПС, является Оператор платежной системы.

(3) Порядок и формы координации деятельности Субъектов платежной системы по обеспечению БФПС и реализации ими мероприятий системы управления рисками.

Порядок и формы координации деятельности Субъектов платежной системы по обеспечению БФПС и реализации ими мероприятий системы управления рисками устанавливает Оператор платежной системы на постоянной основе (с пересмотром порядка и форм координации по мере необходимости).

(4) Порядок и формы осуществления контроля за соблюдением Участниками, Операторами услуг платежной инфраструктуры порядка обеспечения БФПС.

Порядок и формы осуществления контроля за соблюдением Участниками, Операторами услуг платежной инфраструктуры порядка обеспечения БФПС устанавливает Оператор платежной системы на постоянной основе (с пересмотром порядка и форм осуществления контроля по мере необходимости).

(5) Обязанности каждого из привлеченных Операторов услуг платежной инфраструктуры по обеспечению бесперебойности оказания услуг платежной инфраструктуры, предоставляемых им Участникам и их клиентам, а также по организации управления рисками нарушения БФПС в части полномочий, делегированных ему Оператором платежной системы.

Обязанности Операторов услуг платежной инфраструктуры выполняются ими на постоянной основе (с пересмотром их перечня по мере необходимости) в

соответствии с Правилами и законодательством РФ.

(6) Разграничение ответственности и полномочий между Субъектами платежной системы по осуществлению управления рисками нарушения БФПС, в том числе обязанности Оператора платежной системы.

Обязанности Оператора платежной системы, Операторов услуг платежной инфраструктуры и Участников выполняются на постоянной основе (с пересмотром их перечня по мере необходимости) в соответствии с Правилами и законодательством РФ.

(7) Порядок оценки эффективности системы управления рисками Платежной системы в целях ее совершенствования.

Оператор платежной системы анализирует результаты работы Платежной системы с точки зрения влияния на них эффективности системы управления рисками (по мере необходимости, но не реже 1 раза в год).

**5.11.2. Требования к содержанию деятельности по обеспечению БФПС осуществляемой Оператором платежной системы, Операторами услуг платежной инфраструктуры, прямыми и косвенными Участниками**

Требования к содержанию деятельности по обеспечению БФПС, осуществляемой Оператором платежной системы, Операторами услуг платежной инфраструктуры, прямыми и косвенными Участниками, определяются в Правилах и внутренних документах Оператора платежной системы, Операторов услуг платежной инфраструктуры и Участников. Такие требования должны включать:

(1) требования к детализации приемлемого уровня рисков нарушения БФПС в разрезе категорий Субъектов платежной системы:

- Операторов услуг платежной инфраструктуры - по видам услуг;
- Участников - по видам участия в Платежной системе;

(2) порядок разработки, применения и оценки эффективности методик анализа рисков в Платежной системе, требования к оформлению и проверке результатов анализа;

(3) порядок оценки качества и надежности функционирования информационных систем, операционных и технологических средств, применяемых Операторами услуг платежной инфраструктуры;

(4) порядок выбора и реализации мероприятий и способов достижения и поддержания приемлемого уровня рисков нарушения БФПС, порядок оценки их эффективности и совершенствования;

(5) требования к мониторингу рисков нарушения БФПС;

(6) требования к планам обеспечения непрерывности деятельности и восстановления деятельности Операторов услуг платежной инфраструктуры.

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

Порядок информационного взаимодействия Субъектов платежной системы и документационного обеспечения их деятельности по обеспечению БФПС включает:

- перечень документов, используемых Субъектами платежной системы при

осуществлении деятельности по обеспечению БФПС, и порядок их составления;

- порядок информирования Оператора платежной системы о событиях, вызвавших спорные, нестандартные и чрезвычайные ситуации, включая случаи системных сбоев, результатах расследования указанных событий, анализа их причин и последствий;
- порядок информирования Оператора платежной системы о неисполнении или ненадлежащем исполнении обязательств Участников;
- порядок сбора, документирования и статистической обработки первичной информации о функционировании Платежной системы.

Деятельность по обеспечению безопасности функционирования Платежной системы осуществляется Субъектами платежной системы в соответствии с порядком обеспечения БФПС и контролируется Оператором платежной системы.

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

### 5.11.7. Показатели БФПС

К Показателям БФПС относятся:

1. показатель продолжительности восстановления оказания услуг платежной инфраструктуры (далее – «**показатель П1**»), характеризующий период времени восстановления оказания услуг Операторами услуг платежной инфраструктуры в случае приостановления оказания услуг платежной инфраструктуры, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Положением № 382-П;

2. показатель непрерывности оказания услуг платежной инфраструктуры (далее – «**показатель П2**»), характеризующий период времени между двумя последовательно произошедшими Инцидентами, в результате которых приостанавливалось оказание услуг платежной инфраструктуры;

3. показатель соблюдения регламента (далее – «**показатель П3**»), характеризующий соблюдение Операторами услуг платежной инфраструктуры времени начала, времени окончания, продолжительности и последовательности процедур, выполняемых Операторами услуг платежной инфраструктуры при оказании операционных услуг, услуг платежного клиринга и расчетных услуг, предусмотренных частями 3 и 4 статьи 17, частью 4 статьи 19 и частями 1 и 8 статьи 25 Закона о НПС (далее – «**Регламент выполнения процедур**»);

4. показатель доступности Операционного центра (далее – «**показатель П4**»), характеризующий оказание операционных услуг Операционным центром;

5. показатель изменения частоты Инцидентов (далее – «**показатель П5**»), характеризующий темп прироста частоты Инцидентов.

### 5.11.8. Расчет Показателей БФПС

1. Показатель П1 рассчитывается по каждому из Операторов услуг платежной инфраструктуры и по каждому из Инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры, как период времени с момента приостановления оказания услуг платежной инфраструктуры вследствие Инцидента, произошедшего у Оператора

услуг платежной инфраструктуры, и до момента восстановления оказания услуг платежной инфраструктуры.
При возникновении Инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры одновременно двумя и более Операторами услуг платежной инфраструктуры, показатель П1 рассчитывается как период времени с момента приостановления оказания услуг платежной инфраструктуры в результате первого из возникших Инцидентов и до момента восстановления оказания услуг платежной инфраструктуры всеми Операторами услуг платежной инфраструктуры, у которых возникли Инциденты.

Показатель П1 рассчитывается в часах/минутах/секундах.

Показатель П2 рассчитывается по каждому из Операторов услуг платежной инфраструктуры при возникновении каждого из Инцидентов, повлекших приостановление оказания услуг платежной инфраструктуры, как период времени между двумя последовательно произошедшими у Оператора услуг платежной инфраструктуры Инцидентами, в результате которых приостанавливалось оказание услуг платежной инфраструктуры, с момента устранения первого Инцидента и до момента возникновения следующего.

Показатель П2 рассчитывается в часах/минутах/секундах.

2. Показатель П3 рассчитывается по каждому Оператору услуг платежной инфраструктуры.

Для Операционного центра, а также для Платежного клирингового центра показатель П3 рассчитывается как отношение количества распоряжений Участников, по которым в течение календарного месяца были оказаны, соответственно, операционные услуги или услуги платежного клиринга без нарушения Регламента выполнения процедур, к общему количеству распоряжений Участников, по которым были оказаны соответственно, операционные услуги или услуги платежного клиринга в течение календарного месяца, рассчитываемое по следующей формуле:

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

где:

$N_{пкц}$ - количество распоряжений Участников, по которым в течение календарного месяца были оказаны операционные услуги без нарушения Регламента выполнения процедур,

$N_{пкц}^{общ}$ - общее количество распоряжений Участников, по которым были оказаны, соответственно, операционные услуги или услуги платежного клиринга в течение календарного месяца.

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

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

где:

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

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

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

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

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

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

где:

$M$ - количество рабочих дней Платежной системы в месяце,

$D_i$ - общая продолжительность всех приостановлений оказания операционных услуг Операционным центром Платежной системы за i-ый рабочий день месяца в минутах,

$T_i$ - общая продолжительность времени оказания операционных услуг в течение i-го рабочего дня в минутах, установленная в соответствии с временным Регламентом функционирования Платежной системы.

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

4. Показатель П5 рассчитывается по Платежной системе в целом и для каждого Оператора услуг платежной инфраструктуры в отдельности как темп прироста среднедневного количества Инцидентов за оцениваемый календарный месяц по отношению к среднедневному количеству Инцидентов за предыдущие 12 календарных месяцев, включая оцениваемый календарный месяц, рассчитываемый по следующей формуле:

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

где:

$КИ_i$ - количество Инцидентов в течение i-го рабочего дня Платежной системы оцениваемого календарного месяца,

$M$ - количество рабочих дней Платежной системы в оцениваемом календарном месяце,

$N$ - количество рабочих дней Платежной системы за 12 предыдущих календарных месяцев, включая оцениваемый месяц.

Показатель П5 рассчитывается ежемесячно в процентах с точностью до одного знака после запятой (с округлением по математическому методу). В случае если за предыдущие 12 календарных месяцев, включая оцениваемый месяц, Инцидентов не было, значение показателя признается равным нулю.

### 5.11.9 Пороговые уровни Показателей БФПС

| **Показатель БФПС** | **Пороговый (критический) уровень** | **Разрешенный уровень** | **Стандартный уровень** |
|---|---|---|---|
| **П1** | Не более 6 часов | 5-6 часов | Менее 5 часов |

| | | | |
|---|---|---|---|
| **П2** | Не менее 12 часов | 12-13 часов | Более 13 часов |
| **П3** | Не менее 98,0% для Операционного центра и Платежного клирингового центра | От 98,0% до 99,8% для Операционного центра и Платежного клирингового центра | От 99,8% для Операционного центра и Платежного клирингового центра |
| | Не менее 99,0% для Расчетного центра | От 99,0% до 99,5% для Расчетного центра | От 99,5% для Расчетного центра |
| **П4** | Не менее 96,0% | От 96,0% до 99,8% | От 99,8% |
| **П5** | Более 11% | От 11% до 10% | Менее 10% |

### 5.12 Выявление закономерностей функционирования Платежной системы

В целях выявления закономерностей функционирования Платежной системы Оператор платежной системы проводит анализ влияния негативных факторов на операции Платежной системы. Анализ влияния негативных факторов на операции Платежной системы позволяет определить приоритетные процессы Платежной системы, подлежащие восстановлению, путем определения наиболее критических функций, на которые возможно негативное воздействие. Приведенная ниже информация собирается и анализируется для каждого процесса по местонахождению и технологическому обеспечению:

- оценка критичности процессов Платежной системы в зависимости от местоположения (название функции, описание и физический адрес);
- оценка влияния негативных факторов на репутацию, а также правовые последствия для Платежной системы в случае утраты критической функции;
- оценка предполагаемого времени восстановления операций, выражаемого в часах или в днях. Рассчитывается как период, в течение которого критическая функция может быть недоступна с последующим существенным воздействием на операционную деятельность;
- определение целевой точки восстановления, которая представляет собой максимально допустимый уровень потери данных;
- выявление возможностей нарушений надлежащего функционирования Платежной системы, разделение указанных нарушений в соответствии с их влиянием на БФПС.

## 5.13. Порядок информационного взаимодействия в соответствии с требованиями по управлению рисками

Применение положений настоящего раздела 5.13 «*Порядок информационного взаимодействия в соответствии с требованиями по управлению рисками*» в отношении Банка России при выполнении им функций Расчетного центра и Центрального платежного клирингового контрагента и НСПК при выполнении им функций Операционного центра и Платежного клирингового центра регулируется законодательством и соответствующими договорами между Оператором платежной системы и соответствующими Операторами услуг платежной инфраструктуры.

Оператор платежной системы не несет ответственность за риск-менеджмент, его организацию, соблюдение требований риск-менеджмента Банком России и НСПК при выполнении ими расчетных, операционных и платежных клиринговых функций.

### 5.13.1. Общие положения

Оператор платежной системы на регулярной основе получает информацию, необходимую для управления рисками, от Операционного центра и Расчётного центра. Оператор платежной системы имеет право также затребовать любую информацию, касающуюся функционирования Платежной системы, от Участников и Операторов услуг платёжной инфраструктуры.

Участники в своих внутренних документах устанавливают порядок информирования Оператора платежной системы о событиях, которые приводят к недостаточной эффективности или чрезвычайным ситуациям, в том числе о случаях сбоя системы, а также о выводах, сделанных после таких событий, вместе с анализом их причин и последствий.

В случае возникновения обстоятельств, которые препятствуют перечислению средств или исполнению авторизации, платежному клирингу или расчетам по платежам, соответствующий Участник должен незамедлительно проинформировать об этом Оператора платежной системы.

Участники должны незамедлительно информировать Оператора платежной системы в письменной форме о любых предполагаемых или подтвержденных случаях утери, кражи или компрометации любых материалов или записей, которые содержат данные об операциях.

Каждый Эмитент должен сообщать обо всех мошеннических операциях, используя имеющийся механизм уведомления о мошенничестве в сроки и порядке, указанном в пункте 5.13.3 Правил.

Участники должны уведомлять Оператора платежной системы о любых изменениях, касающихся функционирования телекоммуникационной инфраструктуры.

Участники должны уведомлять Оператора платежной системы об отмене дублирующих операций.

Расчётный центр должен ежедневно предоставлять сводный отчет обо всех переводах средств, которые были им обработаны в соответствующий день.

Сводный отчет Расчетного центра представляет собой XML извещение об исполнении, направляемое Расчётным центром в электронном виде через Платежный клиринговый центр.

### 5.13.2. Порядок взаимодействия в чрезвычайных ситуациях

При возникновении чрезвычайных ситуаций, событий, влияющих на БФПС, Участники и Операторы услуг платежной инфраструктуры обязаны незамедлительно проинформировать Оператора платежной системы о возникшей чрезвычайной ситуации всеми доступными способами по следующим адресам и телефонам:

Адрес электронной почты: russia@unionpayintl.com

Телефон: +7 (495) 213-11-20

Факс: +7 (495) 213-11-20

Дальнейшие действия Участников и Операторов услуг платежной инфраструктуры определяется Оператором платежной системы индивидуально по каждой возникшей ситуации.

Оператор платежной системы оценивает риск возможных последствий чрезвычайной ситуации, которая может повлиять на БФПС.

Оператор платежной системы при необходимости оповещает всех Участников и Операторов услуг платежной инфраструктуры о возникшей чрезвычайной ситуации.

Оператор платежной системы прилагает все меры по урегулированию ситуации и недопущению сбоя в работе Платежной системы, вплоть до принудительного отключения Участников, создавших чрезвычайную ситуацию, от Платежной системы.

Оператор платежной системы оповещает Участников и Операторов услуг платежной инфраструктуры об устранении чрезвычайной ситуации, влияющей на БФПС.

### 5.13.3. Система формирования и обработки сообщений о случаях мошенничества

#### 5.13.3.1. Ключевые сведения, подлежащие включению в сообщения

Сообщения о мошеннических операциях должны включать в себя, по крайней мере, следующую информацию: номер карты, дата операции, код авторизации (если таковой имеется), название ТСП и код типа мошеннической операции.

#### 5.13.3.2. Сроки

Эмитент информирует Оператора платежной системы о любых мошеннических операциях в следующие сроки:

- в течение 60 дней после даты совершения мошеннической операции;
- в течение 30 дней после даты получения жалобы от держателя карты, если такая жалоба получена в течение 90 дней после даты совершения мошеннической операции;
- в течение 10 рабочих дней после выявления мошеннической операции Эквайрером.

#### 5.13.3.3. Способ направления сообщения

Эмитент вправе направить сообщение о мошеннической операции в адрес Оператора платежной системы посредством пакетного файла или факсимильного сообщения/зашифрованного электронного письма.

- **Сообщение в формате пакетного файла**

  Эмитент вправе сгенерировать пакетный файл, содержащий информацию о мошеннических операциях, в соответствии с Техническими требованиями к

совместимости банковских карт, и передать его Оператору платежной системы. Оператор платежной системы проверяет и обрабатывает предоставленную информацию и генерирует файл подтверждения для Эмитента, направившего сообщение, на ежедневной основе.

Метод изменения или удаления информации о мошеннических операциях аналогичен описанному выше.

- **Ручная обработка**

  В качестве дополнения и резервной копии Эмитент вправе направить сообщение о мошеннической операции в адрес Оператора платежной системы вручную посредством факсимильного сообщения или зашифрованного электронного письма. Эмитент вправе представить Оператору платежной системы Форму запроса на обработку сообщения о мошеннической операции, которая будет зарегистрирована как представление информации о мошеннической операции в систему от имени Эмитента, и в качестве ответа направить подтверждающее сообщение. Кроме того, система формирования и обработки сообщений о случаях мошенничества генерирует файл подтверждения для Эмитента, направившего сообщение, на ежедневной основе.

### 5.13.4. Отчёт по результатам анализа случаев мошенничества

Система формирования и обработки сообщений о случаях мошенничества может периодически в справочных целях генерировать следующие контрольные отчёты о мошеннических операциях для Эмитентов или Эквайреров в соответствии с классификацией мошеннических операций на основании вида мошеннической операции, её характеристик, места совершения и т.п.:

- Ежеквартальный отчёт об обработанных мошеннических операциях – только для Эмитента;
- Ежемесячный отчёт о показателях деятельности Эмитента – только для Эмитента;
- Ежемесячный отчёт о показателях деятельности Эквайрера – только для Эквайрера;
- Ежемесячный отчёт о мониторинге показателей деятельности ТСП – только для Эквайрера.

### 5.13.5. Система информирования об исключённых ТСП

Эквайреры направляют сообщения, содержащие всю информацию о подозрительных ТСП, в систему информирования об исключённых ТСП.

#### 5.13.5.1. Ключевые сведения, подлежащие включению в сообщения

Информация о подозрительном ТСП, представляемая Эквайрером, должна включать в себя следующие позиции: идентификационный номер ТСП, идентификационный номер Эквайрера, юридическое и коммерческое наименование ТСП, юридический адрес, адрес установки POS-терминала, место расположения, номер телефона ТСП, регистрационный номер лицензии ТСП на ведение хозяйственной деятельности, код категории ТСП (MCC), наименование и идентификационный номер принципала, код возврата платежа по спорной операции, действующую дату соглашения с ТСП и дата принудительного расторжения соглашения.

#### 5.13.5.2. Способ направления сообщения

Эквайрер, направляющий сообщение, следует требованиям системы и представляет информацию о ТСП посредством пакетных файлов или в ручном режиме.

Участник, направляющий сообщение, вправе изменять или удалять представленную им информацию о мошеннической операции.

В качестве дополнения и резервной копии Эквайрер вправе представить информацию о ТСП в адрес Оператора платежной системы вручную посредством факсимильного сообщения или зашифрованного электронного письма. Эквайрер вправе представить Оператору платежной системы форму информационного сообщения о рисках, связанных с исключённым ТСП, после чего сотрудники Оператора платежной системы вводят информацию о ТСП в систему от имени Эквайрера.

Порядок ручной обработки информации об исключённых ТСП аналогичен порядку обработки сообщений о мошеннических операциях.

#### 5.13.5.3. Период хранения информации

Информация о подозрительном ТСП хранится в течение 7 лет после её ввода в систему. В течение этого периода право удалить такую информацию из системы имеет только Эквайрер, который её представил.

### 5.13.6. Система управления рисками эквайринга

Оператор платежной системы использует систему управления рисками эквайринга для оказания Эквайрерам содействия в управлении рисками.

Каждый месяц Оператор платежной системы устанавливает ТСП, замеченные в избыточной мошеннической деятельности, и информирует о них Эквайреров. Отчёты по ТСП, превысившим контрольные пороговые значения, направляются Эквайрерам. После этого от Эквайреров может потребоваться принятие корректирующих мер. Если в течение установленного срока не удаётся снизить уровень мошеннической деятельности до контрольных пороговых значений, это может привести к наложению штрафных санкций.

Оператор платежной системы может предоставить подробную информацию о мошеннической операции и обеспечить мониторинг корректирующих мер и эффективности мер по предотвращению мошеннических операций. Эквайреры обязаны приступить к реализации плана действий немедленно после получения соответствующего уведомления.

## 5.14. Оценка рисков и иерархическое управление

### 5.14.1. Оценка рисков

#### 5.14.1.1. Содержание оценки рисков

**Этап подачи заявления об участии в Платёжной системе (рейтинг кредитных рисков)**

На основе результатов рейтинговой оценки достаточности капитала, обеспеченности активов, качества управления, величины доходов, уровня ликвидности и т. д., проведённой регулятором или сторонней рейтинговой организацией, Оператор платежной системы присваивает заявителю рейтинг кредитных рисков UnionPay. В отсутствие данных рейтинговой оценки сторонней рейтинговой организацией, кредитный риск заявителя оценивается экспертами Оператора платежной системы.

**Этап начала деятельности**

- Управление безопасностью ключей

  Для всех операций, предусматривающих введение ПИН-кода, должна проводиться оценка средства аппаратного шифрования.

  Для всех операций, относящихся к жизненному циклу ключей безопасности, должны соблюдаться общие требования двойного контроля, разделения информации между несколькими лицами, осмотрительной передачи, надлежащего технического обслуживания аппаратного обеспечения и своевременного обновления программного обеспечения. В этих целях необходимо разработать и соблюдать правила и регламенты в отношении контроля доступа, тщательного обследования и согласования, подробной регистрации и проведения сотрудниками всех операций под своими настоящими именами.

  Необходимо разработать и надлежащим образом реализовать механизм внутреннего контроля и надзора, а также осуществлять оценку служебных действий и налагать штрафные санкции за несоблюдение требований безопасности.

- Оценка управления рисками, связанными с ведением хозяйственной деятельности

  Перед присоединением к карточным программам Карт UnionPay заявитель обязан пройти оценку рисков в соответствии с Правилами в отношении различных аспектов, включающих, помимо прочего, следующие:

  - управление рисками, связанными с деятельностью Участников;
  - управление безопасностью данных по счетам и операциям;
  - управление деятельностью по противодействию легализации (отмыванию) доходов, полученных преступным путем

  Результаты оценки рисков, связанных с хозяйственной деятельностью заявителя, служат важным фактором, который используется Оператором платежной системы для определения наличия у заявителя способности начать деятельность, связанную с Картами UnionPay.

**Этап ведения текущей деятельности**

- Оценка рисков, связанных с расчётами

  Эквайрер обязан вести досье на каждое ТСП после заключения с ним соответствующего соглашения. Досье ТСП должно включать в себя следующую информацию:

  1) общие сведения о ТСП;
  2) соглашение с ТСП и связанные дополнительные соглашения;
  3) письменные документы о расторжении или намерении расторгнуть соглашение с ТСП.

- Ежегодная оценка рисков

  Оператор платежной системы проводит ежегодную оценку рисков, обращая особое внимание на Участников, имеющих высокие или необычно высокие показатели риска, с целью отслеживания уровня риска, связанного с такими Участниками, а также принимает необходимые меры по управлению рисками и оказывает соответствующие услуги.

#### 5.14.1.2. Использование оценки уровня рисков

Опираясь на результаты оценки рисков, Оператор платежной системы определяет уровень рисков, который служит одним из факторов при принятии решений относительно того:

- может ли заявителю быть присвоен статус Участника;
- нужно ли заявителю предоставить обеспечение в соответствии с пунктом 5.12.3 Правил;
- может ли заявитель запустить одну или несколько карточных программ UnionPay.

#### 5.14.1.3. Меры по контролю рисков

Меры, принимаемые Оператором платежной системы с целью обеспечить надлежащий контроль рисков, включают в себя, помимо прочего, следующее:

- запуск программы обучения методам управления рисками;
- предоставление обеспечения;
- приостановление действия одной или нескольких карточных программ Карт UnionPay;
- начало реализации экстренного плана по устранению возникших рисков.

### 5.14.2. Иерархическое управление кредитными рисками

#### 5.14.2.1. Критерии рейтинговой оценки рисков

Оператор платежной системы проводит анализ кредитных рисков для каждого Участника на основании следующей информации:

- достаточность капитала;
- обеспеченность активов;
- величина доходов;
- уровень ликвидности;
- результаты рейтинговой оценки регулятором или сторонней рейтинговой организацией (если таковые имеются);
- другая необходимая информация.

#### 5.14.2.2. Классификация уровней рисков

В Платежной системе применяются 5 уровней оценки рисков финансового состояния:

- Уровень A: отличное финансовое положение, значительные возможности в плане погашения имеющейся задолженности.
- Уровень B: стабильное финансовое положение, наличие достаточных финансовых ресурсов, внешней поддержки и возможностей в плане погашения имеющейся задолженности. Заёмщик не подвержен влиянию деловой конъюнктуры или других внешних/внутренних факторов.
- Уровень C: приемлемый уровень финансовых ресурсов и внешней поддержки, хорошие возможности в плане погашения имеющейся задолженности. Заёмщик может быть подвержен влиянию деловой конъюнктуры или других внешних/внутренних

факторов.

- Уровень D: недостаточный уровень финансовых ресурсов, внешней поддержки и возможностей в плане погашения имеющейся задолженности. Заёмщик сильно подвержен влиянию деловой конъюнктуры или других внешних/внутренних факторов.
- Уровень E: банки или финансовые учреждения, близкие к банкротству.

### 5.14.3. Резервное обеспечение

- **Условия предоставления обеспечения**

  Участники, которые подпадают под любую из следующих двух категорий, обязаны предоставить обеспечение, если они:

  - имеют рейтинг кредитного риска на Уровне C или ниже;
  - имеют активы, общая стоимость которых составляет менее эквивалента 17 миллиардов долларов США при доле проблемных активов более 20% или коэффициенте достаточности капитала менее 8%.

- **Определение обеспечения**

  Обеспечение для осуществления расчётов может состоять из аккредитивов, банковских гарантий, поручительств, залогов или иного обеспечения, приемлемого для Оператора платежной системы. Обеспечение предоставляется любым Участником, который подпадает под категорию участников, в отношении ежедневных расчётов которых требуются дополнительные меры предосторожности. Предоставленное обеспечение может быть реализовано в качестве компенсации за причитающиеся к оплате расчётные средства, если предоставивший обеспечение Участник оказывается не в состоянии завершить расчёты по межбанковским операциям с использованием Карт UnionPay в соответствии с установленными требованиями. Допустимые виды обеспечения одобряются Оператором платежной системы по его усмотрению.

- **Срок действия обеспечения**

  Срок действия обеспечения составляет не менее 1 года с даты, в которую Участник подписывает соответствующее соглашение о предоставлении обеспечения и фактического его предоставления.

- **Сумма обеспечения**

  Сумма обеспечения составляет не менее среднемесячной суммы расчётов Участника по межбанковским операциям с использованием Карт UnionPay за последние 12 месяцев. В случае предоставления залога, сумма обеспечения рассчитывается как величина, равная 95% стоимости заложенного имущества, и не может составлять менее 85 000 долларов США или эквивалентной суммы в другой валюте.

  Сумма обеспечения нового Эмитента или Эквайрера не может составлять менее 170 000 долларов США или эквивалентной суммы в другой валюте.

- **Предоставление обеспечения**

  При предоставлении обеспечения Участник обязан представить следующие документы:

- если Участник передаёт в залог имущество, он представляет оригинал правоустанавливающего документа;
- если в качестве залогодателя или гаранта (поручителя) выступает сторонняя организация, она представляет копии своих учредительных документов и лицензий (если применимо), доверенности, удостоверения личности уполномоченного лиц и иные документы, запрошенные Оператором платежной системы;
- если в соответствии учредительными документами требуется корпоративное одобрение обеспечения, Участник представляет заверенную копию такого корпоративного одобрения.

- **Передача обеспечения**

  Участник обязан передать Оператору платежной системы все документы, необходимые для установления соответствующего обеспечения.

  Оператор платежной системы оценивает рыночную стоимость обеспечения или курсы иностранных валют по крайней мере один раз в квартал и контролирует уровни кредитного риска эмитентов, выдавших безотзывные аккредитивы.

  Если стоимость обеспечения снижается до суммы, составляющей менее 95% от требуемой стоимости обеспечения, Оператор платежной системы уведомляет Участника о необходимости предоставления дополнительного обеспечения для того, чтобы компенсировать снижение стоимости обеспечения. Участник предоставляет дополнительное обеспечение для покрытия снижения стоимости в течение 1 месяца после получения такого уведомления. Если Участник не предоставляет дополнительное обеспечение, Оператор платежной системы вправе наложить на такого Участника штрафные санкции.

- **Реализация обеспечения**

  Реализация обеспечения происходит в соответствии с условиями соответствующего документа о предоставлении обеспечения и требований применимого законодательства.

  Если средства, вырученные от реализации обеспечения недостаточны для перечисления средств, уплаты процентов и осуществления соответствующих платежей, Оператор платежной системы сохраняет за собой право дальнейшего требования с должника.

- **Прекращение обеспечения**

  Если рейтинг кредитного риска Участника поднимается до Уровня B или выше, и Оператор платежной системы не вносил платежей за Участника в течение предыдущего года, Оператор платежной системы может прекратить предоставленное обеспечение.

## 5.15. Меры по контролю рисков

### 5.15.1. Программа контроля возвратных платежей ТСП

Программа контроля возвратных платежей ТСП вычисляет отношение суммы возвратных платежей к объёму продаж ТСП. Оператор платежной системы использует для контроля за статусом возвратных платежей ТСП показатели «ежемесячная доля суммы возвратных платежей" и "ежемесячное число возвратных платежей». Если в соответствии со

следующими критериями установлено, что деятельность ТСП может причинить ущерб Платёжной системе, на Эквайрера может быть наложен штраф:

- Если ежемесячная доля суммы возвратных платежей превышает 2,5% или ежемесячное число возвратных платежей превышает 50 в течение двух месяцев подряд, Оператор платежной системы направляет Эквайреру, обслуживающему соответствующее ТСП, письменное предупреждение с требованием принять в кратчайшие сроки необходимые меры. Если Эквайрер не представляет план устранения нарушений в установленные сроки, Оператор платежной системы взимает с Эквайрера штрафную неустойку в размере эквивалента 500 долларов США.
- Если ежемесячная доля суммы возвратных платежей превышает 2,5% или ежемесячное число возвратных платежей превышает 50 в течение трёх месяцев подряд, Оператор платежной системы взимает с Эквайрера комиссию за обслуживание возвратных платежей в размере эквивалента 10 долларов США за каждый новый возвратный платёж начиная с четвёртого месяца до тех пор, пока соответствующие показатели не вернутся к нормальным уровням. Это продолжается до тех пор, пока ежемесячная доля суммы возвратных платежей и ежемесячное число возвратных платежей не вернутся к нормальным уровням.

### 5.15.2. Программа контроля ТСП с высоким уровнем риска

Оператор платежной системы выявляет ТСП, проводящие подозрительные или мошеннические операции, и определяет уровень их рисков.

Если ТСП получает статус ТСП с высоким уровнем рисков, и делается вывод о том, что оно может принести ущерб деятельности, связанной с Картами UnionPay, Эквайрерам рекомендуется расторгнуть соглашения о приёме к обслуживанию Карт UnionPay, заключённые с таким ТСП, в течение 10 рабочих дней и в течение 5 рабочих дней с даты расторжения таких соглашений направить соответствующие сведения о таком ТСП в систему информирования об исключённых ТСП.

Если Эквайрер не расторгает соглашение о приёме к обслуживанию Карт UnionPay, заключённое с таким ТСП, в течение указанного выше срока, он несёт ответственность за возмещение сумм возвратных платежей, связанных с мошенническими операциями, о которых сообщили Эмитенты по истечении указанного срока, до тех пор, пока статус рисков такого ТСП не будет восстановлен до нормального уровня.

Если Эквайрер не расторгает соглашение о приёме к обслуживанию Карт UnionPay, заключённое с таким ТСП, в течение указанного выше срока, и через три месяца такое ТСП сохраняет статус «ТСП с высоким уровнем рисков», UnionPay прекращает обслуживание операций по Картам UnionPay, проводимых таким ТСП, проводит выездную проверку Эквайрера и обучение его персонала и взимает с Эквайрера комиссию за проверку и обучение в размере эквивалента 5 000 долларов США.

### 5.15.3. Программа контроля уровня мошенничества Эквайреров

Программа контроля уровня мошенничества Эквайреров выявляет Эквайреров, на долю ТСП которых приходится непропорционально большой объём мошеннических операций в системе. Программа преследует своей целью сокращение объёмов мошеннических действий и связанных с мошенничеством издержек, которые несут Эквайреры Платежной системе UnionPay.

- Если доля мошеннических эквайринговых операций того или иного Участника за

один квартал составляет 150% от средней доли в России, а сумма эквайринговых мошеннических операций за один квартал превышает эквивалента 20 000 долларов США, Оператор платежной системы направляет Эквайреру письменное уведомление с требованием в кратчайшие сроки принять необходимые меры.

- Если Эквайрер не представляет план устранения нарушений в установленные сроки, Оператор платежной системы взимает с Эквайрера штраф за несоблюдение правил в размере эквивалента 500 долларов США.
- Если ежеквартальная доля мошеннических эквайринговых операций того или иного Эквайрера превышает 150% от средней доли в России, а сумма эквайринговых мошеннических операций за один квартал превышает эквивалента 20 000 долларов США в течение двух кварталов подряд, Оператор платежной системы проводит выездную проверку и обучение персонала Эквайрера и взимает с него штраф в размере эквивалента 5 000 долларов США.
- Если ежеквартальная доля мошеннических эквайринговых операций того или иного Эквайрера превышает 150% от средней доли в России, а сумма эквайринговых мошеннических операций за один квартал превышает эквивалента 20 000 долларов США в течение трёх кварталов подряд, Оператор платежной системы взимает с такого Эквайрера штраф в размере эквивалента 10 000 долларов США.
- Если ежеквартальная доля мошеннических эквайринговых операций того или иного Эквайрера превышает 150% от средней доли в России, а сумма эквайринговых мошеннических операций за один квартал превышает эквивалента 20 000 долларов США в течение четырёх кварталов подряд, Оператор платежной системы может лишить Эквайрера права принимать к обслуживанию Карты UnionPay.

### 5.16. Порядок изменения операционных и технологических средств и процедур

Оператор платежной системы вправе изменять операционные и технологические средства и процедуры по своему усмотрению в следующих случаях:

- в случае изменения порядка оказания услуг или вида операций в Платежной системе;
- в случаях, предусмотренных законодательством РФ;
- по требованию Банка России;
- в рамках системы управления рисками;
- в результате проведения оценки качества функционирования операционных и технологических средств, информационных систем.

Порядок изменения операционных и технологических средств и процедур устанавливается Оператором платёжной системы и Операторами услуг платёжной инфраструктуры и включает временной регламент внедрения изменений. Срок, отводимый на изменение процедур, должен составлять не менее 4 месяцев, за исключением случаев экстренного внедрения изменений, связанных с предотвращением критических сбоев в работе Платёжной системы.

Применение положений настоящего раздела 5.16 «*Порядок изменения операционных и технологических средств и процедур*» в отношении Банка России при выполнении им функций Расчетного центра и Центрального платежного клирингового контрагента и НСПК при выполнении им функций Операционного центра и Платежного клирингового центра регулируется законодательством и соответствующими договорами, заключенным между Оператором платежной системы и соответствующими Операторами услуг платежной инфраструктуры.

Оператор платежной системы не несет ответственность за риск-менеджмент, его организацию, соблюдение требований риск-менеджмента Банком России и НСПК при выполнении ими расчетных, операционных и платежных клиринговых функций.

### 5.17. Порядок оценки качества функционирования операционных и технологических средств, информационных систем

Оценка качества функционирования операционных и технологических средств, информационных систем (в том числе и независимой организацией) проводится в порядке, установленном разделом 4.3 Правил.

# Глава 6. Порядок перевода денежных средств и осуществления платежного клиринга и расчетов

## 6.1. Формы безналичных расчетов, применяемые в Платежной системе

В Платежной системе в соответствии с требованиями Положения 383-П могут применяться следующие формы безналичных расчетов:

- перевод денежных средств по требованию получателя средств (прямое дебетование);
- расчеты платежными поручениями; и
- перевод электронных денежных средств.

Межбанковские расчеты осуществляются в соответствии с законодательством РФ.

## 6.2. Порядок осуществления перевода денежных средств в рамках Платежной системы

Для целей настоящего раздела под термином “Держатель карты” понимаются клиенты Участников – физические лица, индивидуальные предприниматели и юридические лица, являющиеся таковыми в соответствии с законодательством РФ.

Участники осуществляют перевод денежных средств по банковским счетам и(или) без открытия банковских счетов следующими способами:

- списание денежных средств с банковского счета плательщика и зачисление денежных средств на банковские счета получателя платежа (в том числе посредством привлечения банков-посредников), в т.ч. в рамках Перевода с Карты на Карту, на основании распоряжений Держателей карт, составленных с использованием электронного средства платежа, в т.ч. с использованием Карт UnionPay;
- списание денежных средств с банковского счета плательщика и увеличение остатка электронных денежных средств получателя платежа на основании распоряжений Держателей карт, составленных с использованием электронного средства платежа, в т.ч. с использованием Карт UnionPay. Такой порядок перевода денежных средств применяется при переводе денежных средств в рамках одного Участника, а также для электронных платежей внутри Платежной системы;
- списание денежных средств с банковского счета плательщика осуществляется Участником в целях снятия наличных денежных средств физическими лицами-держателями Карт UnionPay;
- уменьшение остатка электронных денежных средств плательщика и зачисление денежных средств на банковский счет получателя платежа (в том числе посредством привлечения банков-посредников) на основании распоряжения Держателя карты-физического лица, составленного с использованием электронного средства платежа, в т.ч. с использованием предоплаченных платежных карт;
- уменьшение остатка электронных денежных средств плательщика и выдача наличных денежных средств Держателям карт-физическим лицам на основании распоряжений таких Держателей карт-физических лиц, составленных с использованием электронного средства платежа, в т.ч. с использованием предоплаченной платежной карты. Указанный порядок перевода допускается только для персонифицированных электронных средств платежа;
- уменьшение остатка электронных денежных средств плательщика с одномоментным увеличением остатка электронных денежных средств получателя платежа на основании

электронных распоряжений Держателей карт, составленных с использованием электронного средства платежа, в т.ч. с использованием предоплаченной платежной карты. Указанный порядок перевода применяется как при переводах в рамках одного Участника, так и при переводе денежных средств в рамках Платежной системы и допускается только при использовании получателем платежа персонифицированных электронных средств платежа;

- приема наличных денежных средств на основании распоряжения Держателя карты, оформленного с использованием электронных средств платежа (в том числе Платежных карт UnionPay), и зачисления денежных средств на банковский счет получателя средств, в т.ч. в рамках Пополнения Карты (в том числе с использованием банков- посредников).

Операции по переводу денежных средств осуществляются по распоряжению Держателей карт, оформленных с использованием электронных средств платежа (их реквизитов), в том числе Карт UnionPay. Все операции осуществляются с учетом особенностей, указанных в Положении 266-П и требований Правил.

В случае осуществления в рамках Платежной системы перевода электронных денежных средств, порядок таких переводов:

- в части максимальной суммы остатка электронных денежных средств при использовании персонифицированных и не персонифицированных электронных средств платежа;
- в отношении общей суммы переводимых электронных денежных средств с использованием одного не персонифицированного электронного средства платежа в течение календарного месяца;
- в отношении выдачи остатка, его части электронных денежных средств (помимо перевода электронных денежных средств), должен соответствовать требованиям Закона о НПС.

Перевод электронных денежных средств в рамках Платежной системы производится путем одновременного уменьшения остатка электронных денежных средств плательщика в обслуживающем его Участнике и увеличения остатка электронных денежных средств получателя в обсуживающие его Участнике. Расчет платежной клиринговой позиции Участника производится путем включения эквивалента суммы перевода электронных денежных средств в платежные клиринговые позиции Участников, определяемые на нетто-основе. Расчеты по операциям перевода электронных денежных средств производятся в общем порядке в соответствии с Правилами.

При совершении операций может производиться авторизация, идентификация и аутентификация с соблюдением требований законодательства РФ и настоящих Правил.

После совершения операции с помощью Карты UnionPay составляются первичные расчетные документы (чеки, слипы), оформляемые в электронном виде или на бумажном носителе. Данные документы служат основанием для составления и передачи платежных инструкций Держателя карты, направляемых Участниками.

Безотзывность такого перевода денежных средств по распоряжениям Держателей карт наступает с момента списания денежных средств с банковского счета плательщика или с момента предоставления плательщиком наличных денежных средств в целях перевода денежных средств без открытия банковского счета.

Безусловность перевода денежных средств по платежным распоряжениям наступает в момент выполнения всех условий по авторизации и удостоверению операции, идентификации и(или) аутентификации в соответствии с требованиями законодательства РФ.

Окончательность перевода денежных средств по платежным распоряжениям наступает в момент зачисления средств на банковский счет получателя средств (в случае осуществления перевода в рамках одного Участника) либо на счет Участника, обслуживающего получателя средств, или увеличения электронных денежных средств получателя (в случае осуществления перевода электронных денежных средств), либо зачисления эквивалента суммы перевода электронных денежных средств на расчетный счет Участника, обслуживающего получателя средств, открытый в Расчетном центре (в случае списания остатка электронных денежных средств или его части на банковский счет), в соответствии с платежными инструкциями.

Порядок перевода денежных средств между Прямыми участниками и Косвенными участниками определяется подписанным между ними соглашением, без участия Оператора платежной системы как стороны по договору.

Среди указанных в настоящем пункте 6.2 способов перевода денежных средств следующие способы позволяют клиентам отправлять денежные средства на собственную Карту UnionPay или иному лицу, являющемуся держателем Карты UnionPay (далее – «**P2P Операция**»):

- Перевод с Карты на Карту;
- Пополнение Карты;
- списание денежных средств с банковского счета плательщика и зачисление денежных средств на счет Получателя на основании распоряжений Держателей карт;
- списание денежных средств с банковского счета плательщика и увеличение остатка электронных денежных средств счета Получателя на основании распоряжений Держателей карт, составленных с использованием электронного средства платежа;
- уменьшение остатка электронных денежных средств плательщика и зачисление денежных средств на счет Получателя на основании распоряжения Держателя карты; и
- уменьшение остатка электронных денежных средств плательщика с одномоментным увеличением остатка электронных денежных средств счета Получателя на основании электронных распоряжений Держателей карт, составленных с использованием электронного средства платежа, в т.ч. с использованием предоплаченной платежной карты.

P2P Операции могут быть совершены только физическими лицами на территории Российской Федерации.

В рамках P2P Операций Эквайреры (для целей настоящего раздела – «**P2P Эквайрер**») обязаны информировать плательщика (в т.ч. Отправителя) до момента осуществления им P2P Операции об установленном Оператором платежной системы размере максимальной суммы по Операциям P2P.

Сумма денежных средств, которую плательщик (в т.ч. Отправитель) может перевести Получателю в рамках P2P Операции, не должна превышать 600 000 (шестьсот тысяч) рублей в день или его эквивалент.

Максимальная сумма одной P2P Операции составляет 150 000 (сто пятьдесят тысяч) рублей.

P2P Эквайреры вправе устанавливать дополнительные ограничения по максимальной сумме P2P Операций.

При проведении P2P Операций с предоплаченными платежными картами Эмитенты должны проводить идентификацию отправителя денежных средств (если применимо) и Получателя денежных средств. Проведение P2P Операций без указанной идентификации запрещено.

### 6.3. Осуществление платежного клиринга и расчетов в Платежной системе с Участниками

Платежный клиринговый центр осуществляет клиринг платежных распоряжений Участников и осуществляет расчет сумм, которые каждый Участник должен каждому другому Участнику путем осуществления платежного клиринга в соответствии с настоящими Правилами и Правилами НСПК.

Расчетный центр осуществляет функции Центрального платежного клирингового контрагента. Особенности осуществления платежного клиринга и расчетов с участием Расчетного центра определяются в соответствующих договорах между Оператором платежной системы и соответствующими Операторами услуг платежной инфраструктуры.

Каждый Прямой участник открывает банковский счет в Расчетном центре. Каждый Косвенный участник открывает счет у Прямого участника и должен осуществить расчеты через Прямого участника.

Каждый Участник будет проинформирован о своих обязательствах Операционным центром в ежедневном отчете о деятельности, содержащем платежную клиринговую позицию Участника и консолидированную информацию о деятельности за предыдущие 24 часа. Участники должны обеспечить наличие на своих счетах в Расчетном центре достаточных средств для покрытия их обязательств по расчетам.

Расчетный центр исполняет поступившие от Платежного клирингового центра распоряжения Участников посредством списания и зачисления денежных средств по банковским счетам Участников. После исполнения таких распоряжений Расчетный центр направляет подтверждения Участникам в порядке, предусмотренном заключенными между ними договорами.

Взаимные требования и обязательства, по которым проводятся расчеты на нетто-основе в Платежной системе, могут быть только между Участниками и Платежной системой. Проведение прямых расчетов между Участниками в Платежной системе не предусмотрено.

Участники должны обеспечить достаточность средств на их Расчетных счетах для покрытия Платежных клиринговых позиций и осуществления исполнений распоряжений Расчетным центром. Если на банковском счете Участника, открытом в Расчетном центре, по состоянию на 24:00 дня Т недостаточно денежных средств для исполнения распоряжения Расчетным центром, Участник обязан немедленно сообщить об этом Оператору платежной системы.

Если на банковском счете Участника, открытом в Расчетном центре, по состоянию на 13:00 дня Т+1 недостаточно денежных средств для исполнения распоряжения Расчетным центром, участие Участника в Платежной системе может быть прекращено по инициативе Оператора платежной системы. Любое возобновление участия Участника возможно только с письменного согласия Оператора платежной системы. В случае, если Оператор платежной системы или UnionPay International, действующее в соответствии с договором с Банком России о предоставлении обеспечения, предоставляет такое обеспечение и покрывает Непокрытую позицию и уплачивает соответствующие суммы штрафов и обеспеченные требования Банка России, Участник обязуется возместить такую сумму, фактически заплаченную Банку России Оператором платежной системы или UnionPay International соответственно, в полном размере. В этом случае Участник также уплачивает Оператору платежной системы неустойку в соответствии с разделом 6.6 Правил.

Распоряжение Платежного клирингового центра представляет собой сообщение, направляемое Платежным клиринговым центром в Расчётный центр, содержащее реестр нетто-позиций.

### 6.4. Процедура перевода денежных средств

Платежный клиринговый центр направляет электронный файл распоряжений в Расчетный центр с

использованием криптографических средств защиты информации для предотвращения проведения несанкционированных манипуляций с распоряжениями Участников.

При получении электронного файла распоряжений Расчетный центр проверяет, что платежные распоряжения составлены в соответствии с Положением 383-П и вся необходимая информация присутствует.

Расчетный центр дебетует или кредитует счет Участника в соответствии с суммой, указанной в платежном распоряжении.

Расчетный центр направляет каждому Участнику выписку на конец рабочего дня, которая включает все платежные распоряжения, обработанные за соответствующий день по счету Участника.

Электронный файл распоряжений означает реестр нетто-позиций, оформленный в электронном виде.

### 6.5. Временной регламент функционирования платежной системы

Проведение авторизаций в Платежной системе обеспечивается Операционным центром в круглосуточном режиме без выходных.

Платежный клиринг в Платежной системе производится ежедневно в рамках единой клиринговой сессии. Центральный процессинговый день (ЦПД или День Т) – день приема к обработке платежных распоряжений Участников Платежным клиринговым центром.

При проведении платежного клиринга по распоряжениям Участников применяется шкала времени по Московскому времени (МТ) в зависимости от типа операции (День Т).

Подлежащие исполнению распоряжения Участников должны быть переданы в телекоммуникационную систему НСПК для последующей передачи Платежному клиринговому центру не позднее 09:00 МТ. Распоряжения, принятые после указанного времени, обрабатываются НСПК на следующий день.

Регламент обработки платежных распоряжений в ЦПД указан в следующей таблице:

| Событие | Время и дата |
|---|---|
| Получение реестров платежей и отчетности (исходящие реестры) | до 09:00 МТ (День Т) |
| Расчет Платежных клиринговых позиций | до 24:00 МТ (День Т) |
| Направление Реестра нетто-позиций в Расчетный центр для исполнения | до 12:00 МТ (День Т+1) |
| Осуществление Расчетным центром расчетов между Участниками на основании Реестра нетто-позиций | до 13:00 МТ (День Т+1) |

Операции, осуществляемые Платежным клиринговым центром и Расчетным центром, должны быть осуществлены Платежным клиринговым центром и Расчетным центром в сроки, установленные соглашениями между Оператором платежной системы, Платежным клиринговым центром и Расчетным центром в отношении осуществления соответствующих функций.

### 6.6. Комиссия за несвоевременные расчеты

Если на банковском счете Участника, открытом в Расчетном центре, недостаточно денежных средств для исполнения распоряжения Расчетным центром, неустойка в размере 0,05% от суммы несвоевременного расчета за каждый календарный день будет снята и перечислена Оператору платежной системы (в дополнение к убыткам, причиненным Оператору платежной системы).

### 6.7. Особенности перевода денежных средств и осуществления платежного клиринга в рамках Перевода с Карты на Карту и Пополнения Карты

Для целей настоящего раздела подлежат применению положения, предусмотренные разделами 6.1-6.6. Правил.

Операция Перевода с Карты на Карту состоит из двух частей:

- списания денежных средств с Отправителя (далее – «**Операция списания**»);
- зачисления денежных средств Получателю (далее – «**Операция зачисления**»).

Операция Пополнения Карты состоит из Операции зачисления.

Операция списания подлежит передаче P2P Эквайрером на платежный клиринг в срок, не превышающий 7 (семи) календарных дней после даты получения авторизации по Операции списания.

Операция зачисления не подлежит передаче на платежный клиринг.

В рамках Перевода с Карты на Карту Эмитент обязан сделать денежные средства доступными для Получателя сразу после проведения авторизации по Операции зачисления.

P2P Эквайреры вправе взимать дополнительное комиссионное вознаграждение с Отправителя в рамках Перевода с Карты на Карту. В таком случае P2P Эквайреры обязаны информировать Отправителя до момента осуществления им Перевода с Карты на Карту о размере комиссионного вознаграждения, взимаемого с Отправителя за совершение указанной Операции. Отправителю должна предоставляться возможность отказа от совершения им Операции Перевода с Карты на Карту после ознакомления с информацией о размере комиссионного вознаграждения, взимаемого P2P Эквайрером. При этом сумма комиссионного вознаграждения должна быть указана в первичном документе, выдаваемом Отправителю.

P2P Эквайрер вправе отменить Операцию списания в рамках Перевода с Карты на Карту, ранее направленную на платежный клиринг, только в целях исправления ошибок обработки данных по Операции. P2P Эквайрер обязан направить на платежный клиринг отмену Операции списания в течение 45 (сорока пяти) календарных дней с даты обработки Операции.

Отмена Операции зачисления запрещена.

# Глава 7. Разрешение споров

## 7.1. Общие положения

### 7.1.1. Тщательное и своевременное рассмотрение

Оператор платежной системы, Операторы услуг платежной инфраструктуры и Участники обязуется урегулировать возникающие между ними споры добросовестно и своевременно.

### 7.1.2. Взаимное содействие

Участник обязуется назначать специальных работников для управления процедурой урегулирования споров и стремиться оказывать содействие другим Участникам в урегулировании споров между следующими сторонами:

- Держателем карты и ТСП другого Участника;
- ТСП и Держателем карты другого Участника;
- в урегулировании любых других споров между Участниками, Оператором платежной системы и Операторами услуг платежной инфраструктуры.

При урегулировании споров любые документы или файлы/чеки, которые могут подтвердить/доказать подлинность операции, могут считаться приемлемой заменой стандартных квитанций/документов, предусмотренных Правилами.

Эмитент обязан по запросу (в том числе, повторному запросу) в течение установленного периода времени предоставлять чеки и иные документы по операциям по выпущенным им Картам UnionPay за последние 12 месяцев даже в том случае, если у Эмитента отсутствует обязательство по обратному зачислению средств.

Участнику разрешается получить только невыплаченный остаток по операции (за исключением особых обстоятельств, таких как возвраты платежей в связи с начислением штрафов). Если Эмитент успешно инициировал возврат платежа, денежные средства должны быть зачислены на счет Держателя карты в течение установленного периода времени.

Маршрутизация операции по урегулированию споров должна соответствовать маршрутизации первоначальной операции.

При возникновении разногласий между Участниками по внутринациональным операциям, Участники для обмена соответствующей документацией обязаны использовать систему электронного документооборота СЭДО НСПК в соответствии с регламентами использования СЭДО НСПК, опубликованными НСПК.

## 7.2. Арбитраж

Арбитраж позволяет UnionPay установить, кто несет ответственность за спорную операцию в тех случаях, когда ситуацию не удается урегулировать с помощью операции возврата платежа по спорным операциям и повторного предъявления к оплате. Условия и требования к процедуре арбитража изложены в Операционных правилах платежной системы UnionPay International.

Если Эмитент считает необоснованным повторное предъявление к оплате, выставленное Эквайрером, он имеет право подать заявление об урегулировании спорного вопроса с помощью арбитража, в котором в качестве арбитра будет выступать UnionPay. В ходе процедуры арбитража UnionPay принимает решение о том, какая из сторон несет ответственность за спорную операцию.

Решение UnionPay является окончательным и в качестве такового должно быть принято Эмитентом и Эквайрером, за исключением тех случаев, когда имеются законные основания для его обжалования. В ходе процедуры арбитража комиссия по арбитражу и урегулированию спорных ситуаций проверяет все документы и данные, предоставленные обоими Участниками, чтобы определить, кто несет окончательную ответственность за спорную операцию. Подающий заявление Участник обязан возместить любую разницу между суммой, изначально предъявленной к оплате, и суммой возвратного платежа или суммой, указанной в повторном предъявлении к оплате, причиной которой является изменение курсов валют.

### 7.3. Досудебное урегулирование споров

В случае возникновения споров между Участниками и Оператором платежной системы, заявившая сторона должна уведомить об этом другую сторону спора в течение 30 календарных дней с момента наступления события, вследствие которого возник такой спор. Заявившая сторона должна представить другой стороне спора все необходимые сопутствующие документы и доказательства в обоснование своей позиции вместе с уведомлением о возникновении спорной ситуации.

В течение 60 календарных дней после получения уведомления получатель проводит расследование и направляет ответ инициирующей спор стороне. Получатель и заявившая сторона предпримут все меры для урегулирования спора путем переговоров. В случае невозможности урегулирования спора путем переговоров получатель и заявившая сторона должны в течение 30 календарных дней после ответа получателя на уведомление о возникновении спорной ситуации обсудить и принять решение по мерам урегулирования спорной ситуации, включая рассмотрение спора в судебном порядке.

В случае возникновения споров между Оператором услуг платежной инфраструктуры и Оператором платежной системы, спор разрешается в порядке, установленном в соответствующих соглашениях, заключенных между ними. В случае возникновения споров между Участником и Оператором услуг платежной инфраструктуры, спор разрешается в порядке, установленном в Правилах и соответствующих соглашениях, заключенных между ними.

# Глава 8. Порядок оплаты услуг

## 8.1. Порядок оплаты услуг Участников по переводу денежных средств их клиентами

Услуги Участников по переводу денежных средств оплачиваются Держателями карт и ТСП Участникам в наличной или безналичной форме на основании заключённых между ними договоров, которые не могут предусматривать минимального размера оплаты услуг по переводу денежных средств, а также должны обеспечивать единообразный порядок оплаты услуг по переводу денежных средств.

## 8.2. Порядок оплаты услуг Оператора платежной системы

Все денежные сборы, взимаемые Оператором платежной системы, будь то в форме комиссий, курсов обмена валют или в какой-либо другой форме, взимаются с Участников. Участник несет ответственность за уплату всех денежных сборов, вне зависимости от того, оплачивает ли он их самостоятельно, передает другой стороне или увеличивает их сумму при выставлении счета своим клиентам.

Информация о размерах действующих комиссий приведена в положении о сборах и комиссиях по Картам UnionPay, которое находится в открытом доступе в сети Интернет на сайте Оператора платежной системы www.unionpayintl.com. Положение о сборах и комиссиях по Картам UnionPay является неотъемлемой частью Правил. Оператор платежной системы вправе в одностороннем порядке пересматривать размер комиссий и сборов по правилам раздела 1.3 Правил.

В соответствии с ч. 8.1 ст. 20 Закона о НПС, при внесении изменений в Правила, предусматривающих введение новых тарифов или увеличение размера тарифов, Оператор платежной системы обязан уведомить об этом Банк России в срок не менее чем за 30 календарных дней до дня введения в действие изменений в правила платежной системы с предоставлением расчетов, обосновывающих указанные изменения.

Оператор платежной системы ежемесячно не позднее 15-го календарного месяца, следующего за отчетным, выставляет на каждого Участника счет и акт оказания услуг за отчетный месяц. Счета и акты оказания услуг направляются Прямым участникам вместе со счетами и актами оказания услуг косвенных Участников, открывших счет у такого Прямого участника. Копии счетов могут также быть предоставлены через систему электронного информирования или по электронной почте.

Оператор платежной системы не позднее 15-го числа месяца, следующего за отчетным, направляет распоряжения в Расчетный центр на списание сумм, указанных в счетах. Каждый Прямой Участник настоящим предоставляет Оператору платежной системы право списывать с его банковских счетов, открытых в Расчетном центре, каждую сумму, которую он должен уплатить Оператору платежной системы за оказанные услуги на основании выставленных Оператором платежной системы счетов. Порядок такого списания регулируется соответствующими соглашениями между Оператором платежной системы, Расчетным центром и Участниками.

Участник в течение 10-ти календарных дней со дня получения документов подписывает акт оказания услуг и возвращает один экземпляр акта Оператору платежной системы. В случае несогласия с суммой счета, Участник вправе оспорить суммы учета в течение 10-ти календарных дней со дня получения документов. В случае согласования изменения суммы счета Оператором платежной системы, корректировка производится в следующем отчетном периоде.

Порядок оплаты услуг Оператора платежной системы Участниками является единообразным для всех Участников.

### 8.3. Порядок оплаты услуг платежной инфраструктуры

Оплата услуг Операторов услуг платежной инфраструктуры будет производиться Оператором платежной системы на основании ежемесячных счетов в соответствии с заключенными договорами. Участники не оплачивают услуги Операторов услуг платежной инфраструктуры.

### 8.4. Оплата услуг Расчетного центра

В рамках Платежной системы не установлены отдельные тарифы за услуги Расчетного центра, оказываемые в рамках платежной системы.