УТВЕРЖДЕНО

АО «ПейТех»
(Приказ № 2 от 26 «августа» 2024 года)

Генеральный директор
Балакин И.И.

26 «августа» 2024 года

ПРАВИЛА
Международной платежной системы денежных переводов «Омнипэй»

Москва 2024 г.

ОГЛАВЛЕНИЕ

Глава 1. Общие положения

1.1 Платежная Система «Омнипэй»

1.1.1. Международная платежная система денежных переводов «Омнипэй» представляет собой совокупность организаций, объединенных единым информационным пространством и осуществляющих перевод денежных средств между странами присутствия Международной системы денежных переводов «Омнипэй» (далее «**Система» или «Платежная Система»**). Платежная Система создана в Российской Федерации и действует в соответствии с требованиями Федерального закона № 161-ФЗ «О национальной платежной системе», а также в соответствии с нормативными актами Банка России. За пределами Российской Федерации Платежная Система осуществляет свою деятельность с учетом требований законодательства стран осуществления деятельности.

1.2 Правила Платежной Системы

1.2.1 Настоящие Правила Платежной Системы (далее «**Правила**»), включая все Приложения, составлены в соответствии с положениями законодательства Российской Федерации, а также политиками и процедурами Системы и представляют собой единый документ, устанавливающий условия участия в Платежной Системе, условия осуществления перевода денежных средс тв в рамках Платежной Системы, порядок оказания услуг платежной инфраструктуры, а также иные условия, определенные настоящими Правилами.

1.2.2 Для целей настоящих Правил под законодательством Российской Федерации понимаются все законы и нормативные акты, действующие в Российской Федерации, в том числе нормативные акты Банка России.

1.3 Термины и определения:

Аннулирование перевода денежных средств – аннулирование распоряжения отправителя с последующим возвратом денежных средств отправителю;

Банковский Платежный Агент (Агент) – юридическое лицо, за исключением кредитной организации, или индивидуальный предприниматель, который привлекается Участником в соответствии с законодательством Российской Федерации, настоящими Правилами и договором между Участником и Агентом в целях осуществления отдельных банковских операций от имени Участника;

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

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

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

Интернет-банк – способ удаленного осуществления перевода денежных средств клиентом Участника через Интернет с использованием автоматизированной системы Участника, при котором денежные средства списываются со счета клиента Участника, открытого у Участника, или зачисляются на счет клиента Участника, открытый у Участника;

Контрольный Номер Денежного Перевода (КНДП) – номер, присваиваемый процессингом Платежной Системы каждому переводу денежных средств при его отправлении и являющийся одним из реквизитов перевода;

Окончательность перевода денежных средств – характеристика перевода денежных средств,

обозначающая предоставление денежных средств получателю средств в определенный момент времени (с учетом положений части 10 статьи 5 Федерального закона от 27.06.2011 № 161-ФЗ «О национальной платежной системе»);

Оператор Платежной Системы (Оператор) – организация, определяющая Правила, а также выполняющая иные функции оператора платежной системы, предусмотренные законодательством Российской Федерации и настоящими Правилами;

Операторы Услуг Платежной Инфраструктуры (Оператор УПИ) – Операционный Центр (ОЦ), Центральный Платежный Клиринговый Контрагент (ЦПКК) и Расчетный Центр (РЦ);

Операционный Центр (ОЦ) – организация, предоставляющая в рамках Платежной Системы Операционные Услуги;

Операционные Услуги – деятельность Операционного Центра в рамках Платежной Системы по обеспечению Участникам и их клиентам доступа к Услугам, а также обмену электронными сообщениями;

Отделение – любой офис продаж Участника (в том числе офис продаж, привлеченного Участником Агента);

Партнер Платежной Системы (Партнер) – организация, уполномоченная в соответствии с законодательством страны местонахождения осуществлять операции по переводу денежных средств, и осуществляющая:

- отправку переводов денежных средств для выплаты с использованием Платежной Системы;

и (или)

- выплату переводов денежных средств, поступивших с использованием Платежной Системы.

Взаимодействие между Партнерами и Платежной Системой осуществляется на основании договора между Участником и Партнером, действующим в качестве клиента Участника.

Плата за перевод – плата за оказание клиентам услуг по переводу денежных средств, взимаемая с клиентов – отправителей переводов денежных средств и (или) клиентов – получателей переводов денежных средств. Плата за перевод, устанавливается Оператором;

Поручение на осуществление выплаты денежных средств (ПОВДС) – поручение на осуществление выплаты перевода денежных средств, передаваемое получателем Участнику (в том числе в электронном виде, если применимо), содержащее обязательные реквизиты перевода денежных средств и являющееся основанием для выплаты перевода денежных средств получателю;

Поручение на осуществление перевода денежных средств (ПОПДС) – поручение на осуществление перевода денежных средств в пользу физического или юридического лица в рамках Платежной Системы, передаваемое отправителем Участнику (в том числе в электронном виде, если применимо) и являющееся договором между отправителем и Участником;

Расчетный Центр (РЦ) – организация, созданная в соответствии с законодательством Российской Федерации, предоставляющая в рамках Платежной Системы Расчетные Услуги;

Расчетные Услуги – деятельность Расчетного Центра в рамках Платежной Системы по обеспечению исполнения распоряжений Участников посредством списания и зачисления денежных средств по банковским счетам Участников, а также направлению подтверждений, касающихся исполнения распоряжений участников Платежной Системы;

СПК – справочно-информационная служба поддержки клиентов Платежной Системы.

Субъект – любой субъект Платежной Системы, включая Оператора, любого Оператора УПИ, Участника и Партнера.

Терминал самообслуживания – техническое средство или программный комплекс, позволяющие отправлять и (или) выплачивать переводы денежных средств в автоматическом режиме (в том числе сайт в сети Интернет, банкомат или платежный терминал);

Условия оказания Услуги – устанавливаемые Оператором общие условия, на которых Услуга оказывается клиентам Участников;

Услуга – услуга по переводу денежных средств, оказываемая Участниками их клиентам с использованием Платежной Системы, представляющая собой:

а) трансграничные переводы денежных средств физических лиц в пользу физических лиц для выплаты наличными денежными средствами или зачисления на счет;

б) трансграничные переводы денежных средств физических лиц на счета юридических лиц;

в) трансграничные переводы денежных средств со счетов юридических лиц в пользу физических лиц для выплаты наличными денежными средствами или зачисления на счет.

Услуги платежной инфраструктуры (УПИ) – Расчетные Услуги, Операционные Услуг, Услуги Платежного Клиринга;

Услуги Платежного Клиринга – деятельность Центрального Платежного Клирингового Контрагента по обеспечению в рамках Платежной Системы приема к исполнению распоряжений Участников об осуществлении перевода денежных средств и выполнению иных действий, предусмотренных законодательством Российской Федерации или настоящими Правилами;

Участник – российская кредитная организация, являющаяся оператором по переводу денежных средств, присоединившаяся к Правилам и оказывающая Услуги своим клиентам – физическим и юридическим лицам – в соответствии с законодательством Российской Федерации и настоящими Правилами;

Центральный Платежный Клиринговый Контрагент (ЦПКК) – платежный клиринговый центр Платежной Системы, выступающий плательщиком и получателем средств по переводам денежных средств Участников. Центральный Платежный Клиринговый Контрагент предоставляет в рамках Платежной Системы Услуги Платежного Клиринга.

1.4 Сфера действия Правил

1.4.1 Настоящие Правила действуют на территории Российской Федерации. За пределами Российской Федерации настоящие Правила действуют в части, не противоречащей нормам международного законодательства, законам и нормативно-правовым актам иностранных государств, на территории которых оказывается Услуга, и условиям двусторонних договоров, заключенных Оператором с Партнерами.

Глава 2. Оператор Платежной Системы

2.1 Общие положения

2.1.1 Оператором Платежной Системы является Акционерное общество «ПейТех», ОГРН 1247700378969. Контактная информация оператора размещается Оператором на сайте www.omnypay.ru.

2.2 Обязанности Оператора

Оператор обязан:

i) определять Правила, организовывать и осуществлять контроль за их соблюдением Участниками и Операторами Услуг Платежной Инфраструктуры;

ii) осуществлять привлечение Операторов Услуг Платежной Инфраструктуры, обеспечивать контроль за оказанием услуг платежной инфраструктуры Участникам, а также вести перечень Операторов Услуг Платежной Инфраструктуры;

iii) организовать систему управления рисками в Платежной Системе в соответствии с требованиями законодательства Российской Федерации и осуществлять оценку и управление рисками в Платежной Системе;

iv) обеспечить бесперебойность оказания услуг платежной инфраструктуры Участниками;

v) информировать Банк России и Участников о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в день такого приостановления (прекращения) в порядке, установленном Банком России;

vi) обеспечить бесперебойность функционирования Платежной Системы в порядке, установленном Банком России;

vii) обеспечить возможность досудебного и (или) третейского рассмотрения споров с

Участниками и Операторами Услуг Платежной Инфраструктуры в соответствии с положениями настоящих Правил;

viii) предоставлять организациям, намеревающимся участвовать в Платежной Системе, Правила для предварительного ознакомления без взимания платы, за исключением расходов на изготовление копий Правил Платежной Системы;

ix) размещать в открытом доступе Правила, на сайте www.omnypay.ru, за исключением требований к защите информации, и информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

x) своевременно информировать Участников об изменениях в настоящих Правилах в соответствии с порядком, установленным настоящими Правилами;

xi) в соответствии с требованиями законодательства Российской Федерации обеспечить защиту и конфиденциальность информации, содержащей персональные данные, банковскую тайну, а также информации, доступ к которой ограничен законодательством Российской Федерации, договором или настоящими Правилами;

xii) осуществлять свою деятельность в соответствии с требованиями законодательства Российской Федерации и настоящими Правилами;

xiii) нести иные обязательства, прямо предусмотренные настоящими Правилами.

2.3 Права Оператора

Оператор имеет право:

i) в одностороннем порядке вносить изменения в настоящие Правила в соответствии с требованиями законодательства Российской Федерации и порядком, предусмотренными настоящими Правилами;

ii) принимать решение о начале или прекращении участия в Платежной Системе отдельных Участников в соответствии с настоящими Правилами;

iii) внедрять новые виды Услуг;

iv) устанавливать и изменять Плату за перевод по всем или отдельным Услугам;

v) определять вознаграждение Участника, причитающееся Участнику за оказание Услуг клиентам Участника с учетом положений Приложения № 8 к настоящим Правилам;

vi) устанавливать и изменять Условия оказания Услуги;

vii) рассматривать жалобы клиентов Участников на действия (бездействие) Участников при оказании Услуги Участниками;

viii) применять к Участникам и Операторам Услуг Платежной Инфраструктуры санкции, предусмотренные настоящими Правилами;

ix) принимать участие в рассмотрении споров между Участниками, а также между Участниками и Операторами Услуг Платежной Инфраструктуры;

x) выносить решения о надлежащем/ненадлежащем оказании Услуги Участником клиенту;

xi) в соответствии с настоящими Правилами устанавливать для каждого Участника лимиты на сумму отправления одного перевода денежных средств или общую сумму переводов денежных средств, отправляемых Участником за определенный период времени из одного Отделения (и/или через Интернет-банк и/или через Терминал самообслуживания) или всех Отделений (и/или через Интернет-банк и/или через Терминал самообслуживания);

xii) требовать от Участника перечисления гарантийного взноса в размере, устанавливаемом Оператором в соответствии с настоящими Правилами;

xiii) устанавливать и изменять требования по защите информации при осуществлении перевода денежных средств;

xiv) устанавливать обязательные для Участников и Операторов Услуг Платежной Инфраструктуры требования по противодействию отмыванию доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения в соответствии с законодательством Российской Федерации и стандартами Системы;

xv) запрашивать и получать информацию от Участников в отношении оказанных ими Услуг;

xvi) запрашивать и получать информацию от Операторов Услуг Платежной Инфраструктуры в отношении оказанных ими Услуг (в случае привлечения Оператором сторонних Операторов Услуг Платежной Инфраструктуры);

xvii) привлекать дополнительных Операторов Услуг Платежной Инфраструктуры;

xviii) пользоваться иными правами, предусмотренными законодательством Российской Федерации и настоящими Правилами;

xix) предоставлять Участникам информационные материалы и их электронные макеты для размещения таких информационных материалов в Отделениях, Интернет-банке и на интернет-сайтах. При этом, при отсутствии иных договоренностей между Оператором и Участником, все информационные материалы, переданные Оператором Участнику, остаются собственностью Оператора.

2.4 Контакты Оператора

2.4.1 По всем вопросам функционирования Платежной Системы Участники и Операторы Услуг Платежной Инфраструктуры могут обращаться к Оператору по телефонам или электронной почте, указанным на сайте Платежной Системы по адресу www.omnypay.ru.

2.4.2 Клиенты Участников обращаются к Оператору в соответствии с положениями Условий оказания Услуги.

Глава 3. Услуга

3.1 Общие положения

3.1.1 Услуга оказывается Участниками их клиентам в соответствии с законодательством Российской Федерации, настоящими Правилами и Условиями оказания Услуги, которые являются неотъемлемой частью настоящих Правил.

3.1.2 При осуществлении переводов денежных средств прием и выдача денежных средств осуществляются Участниками в порядке, предусмотренном настоящими Правилами.

3.1.3 При осуществлении переводов денежных средств прием и выдача денежных средств осуществляются Участниками в российских рублях или долларах США.

3.1.4 Перечень Услуг, оказываемых каждым Участником своим клиентам, определяется Оператором в соответствии с настоящими Правилами.

3.1.5 Перечень стран, в которые возможно отправить перевод денежных средств через Платежную Систему, ведется Оператором и публикуется на сайте Платежной Системы по адресу www.omnypay.ru. Оператор регулярно обновляет соответствующий перечень путем размещения перечня стран на сайте www.omnypay.ru.

3.2 Условия оказания Услуги

3.2.1 Для получения Услуги отправитель перевода денежных средств через Платежную Систему заключает договор с Участником в форме ПОПДС в соответствии с Условиями оказания Услуги, которые являются неотъемлемой частью договора между Участником и отправителем перевода денежных средств.

3.2.2 Условия оказания Услуги устанавливаются Оператором и являются едиными для всех Участников на территории Российской Федерации. Оператор публикует Условия оказания Услуги на сайте www.omnypay.ru. Оператор вправе вносить изменения в Условия оказания Услуги в порядке, предусмотренном настоящими Правилами.

3.2.3 При присоединении к настоящим Правилам Участнику предоставляются Условия оказания Услуги.

3.2.4 Участник обязан обеспечить ознакомление клиента с Условиями оказания Услуги, в том

числе путем размещения Условий оказания Услуги в свободном для клиентов доступе в Отделениях, Интернет-банке или Терминалах самообслуживания Участника, а также получить согласие клиента с Условиями оказания Услуги до момента совершения таким клиентом перевода денежных средств. По требованию Оператора Участник обязан предоставить Оператору копии документов, заверенные Участником и подтверждающие согласие клиента с Условиями оказания Услуги.

3.3 Порядок оказания Услуги

3.3.1 Применяемые формы безналичных расчетов

3.3.1.1 В рамках Платежной Системы применяются следующие формы безналичных расчетов:

а) расчеты платежными поручениями;

б) расчеты в форме перевода денежных средств по требованию получателя (прямое дебетование).

3.3.1.2 Расчеты между Участниками и Оператором осуществляются в рамках Платежной Системы в соответствии с Главой 6 настоящих Правил.

3.3.2 Виды Услуг

В Платежной Системе в Российской Федерации доступны следующие виды Услуг:

а) перевод денежных средств физического лица в пользу физического лица;

б) перевод денежных средств физического лица в пользу юридического лица;

в) перевод денежных средств от юридического лица в пользу физического лица.

Услуги по переводу денежных средств между отправителями и получателями переводов денежных средств, находящимися на территории Российской Федерации, в рамках Платежной Системы не предоставляются.

3.3.2.1 Перевод денежных средств физического лица в пользу физического лица

Перевод денежных средств, отправленный физическим лицом в пользу физического лица, как правило, становится доступен для выплаты получателю в стране получения перевода денежных средств в течение нескольких минут после отправления соответствующего перевода денежных средств. Моментом отправления такого перевода денежных средств считается момент присвоения соответствующему переводу КНДП.

Перевод денежных средств, отправленный физическим лицом в пользу физического лица для выплаты в наличной форме, является переводом до востребования, то есть получатель перевода денежных средств может обратиться за выплатой перевода в любое Отделение на территории Российской Федерации (для переводов денежных средств, отправленных в Российскую Федерацию) или в любой пункт обслуживания Партнера в стране выплаты перевода денежных средств (для переводов денежных средств, отправленных из Российской Федерации). Подтверждением обеспечения возможности выплаты перевода денежных средств в Платежной Системе является присвоение переводу денежных средств КНДП. Для данного способа выплаты перевода денежных средств организация, осуществляющая выплату перевода, определяется получателем в момент обращения за выплатой с учетом требований настоящих Правил.

При осуществлении перевода денежных средств, отправленных физическим лицом в пользу физического лица для зачисления на счет, организация, осуществляющая выплату перевода денежных средств, определяется отправителем такого перевода денежных средств в момент отправления перевода.

Безотзывность перевода денежных средств для данного вида Услуг наступает с момента списания денежных средств с банковского счета отправителя (или с момента уменьшения баланса банковской карты отправителя) или с момента предоставления отправителем наличных денежных средств в целях перевода денежных средств без открытия банковского счета.

Безусловность перевода денежных средств для данного вида Услуг наступает с момента выполнения получателем, обратившимся за выплатой перевода денежных средств, всех условий выплаты перевода в стране назначения перевода денежных средств.

Окончательность перевода денежных средств для данного вида Услуг наступает:

- в момент поступления денежных средств на счет ЦПКК.

Аннулирование перевода денежных средств для данного вида Услуг возможно:

- по заявлению отправителя в любой момент до выплаты перевода денежных средств получателю;

- по инициативе Участника до наступления Безотзывности перевода денежных средств при условии, что перевод денежных средств не выплачен получателю.

В случае Аннулирования перевода денежных средств по заявлению отправителя, возврат перевода денежных средств осуществляется без взимания дополнительной платы. Плата за перевод, внесенная отправителем при отправлении перевода, при Аннулировании перевода денежных средств не возвращается. При этом, Оператор или Участник вправе принять решение о возврате Платы за перевод отправителю при Аннулировании перевода денежных средств. Плата за перевод также может возвращаться при Аннулировании перевода денежных средств в случаях, предусмотренных настоящими Правилами и Условиями оказания Услуги.

Валюты отправления и выплаты переводов денежных средств, а также условия конвертации определяются в соответствии настоящими Правилами.

Плата за перевод при оказании настоящей Услуги взимается во всех случаях с отправителя в соответствии с п. 3.4 настоящих Правил.

3.3.2.2 Перевод денежных средств физического лица в пользу юридического лица

Перевод денежных средств физического лица в пользу юридического лица может быть осуществлен исключительно в адрес юридических лиц – клиентов Участников, зарегистрированных в Платежной Системе в качестве получателей переводов.

Безотзывность и Окончательность перевода денежных средств в рамках данной Услуги наступают по общим правилам наступления Безотзывности и Окончательности перевода денежных средств физического лица в пользу физического лица.

Безусловность перевода денежных средств в рамках данной Услуги наступает с момента наступления Безотзывности перевода денежных средств.

Аннулирование перевода денежных средств и/или внесение изменений в перевод денежных средств в рамках данной Услуги возможно только до момента наступления Безотзывности перевода денежных средств.

3.3.2.3 Перевод денежных средств от юридического лица в пользу физического лица

Перевод денежных средств от юридического лица в пользу физического лица осуществляется исключительно по поручению юридических лиц – клиентов Участников, зарегистрированных в программном обеспечении Платежной Системы.

Безотзывность, и Окончательность перевода денежных средств в рамках данной Услуги наступают по общим правилам наступления Безотзывности, Безусловности и Окончательности перевода денежных средств физического лица в пользу физического лица.

Безусловность перевода денежных средств в рамках данной Услуги наступает с момента наступления Безотзывности перевода денежных средств.

Аннулирование перевода денежных средств и/или внесение изменений в перевод денежных средств в рамках данной Услуги возможно только до момента наступления Безотзывности перевода денежных средств.

Выплата переводов в рамках настоящей Услуги осуществляется по общим правилам выплаты переводов денежных средств.

3.3.3 Способы предоставления доступа к Услугам

3.3.3.1 Участники предоставляют своим клиентам доступ к Услугам следующими способами:

а) непосредственно в Отделениях Участников (их Агентов) с участием сотрудников Участников (их Агентов);

и (или)

б) с использованием программных или программно-аппаратных средств, без непосредственного участия сотрудников, в том числе через Интернет-банк, Терминалы самообслуживания или иные программные или программно-аппаратные средства, позволяющие обеспечивать клиентам Участника доступ к Услугам без непосредственного участия сотрудников Участников (их Агентов).

3.3.3.2 Способ(ы) предоставления Участником доступа своим клиентам к Услугам определяется Оператором при регистрации Участника в Платежной Системе в зависимости от способа реализации доступа Участника к Платежной Системе и технических возможностей Участника.

3.3.4 Валюта

3.3.4.1 В целях оказания Услуги по осуществлению отправления перевода денежных средств из Российской Федерации или по выплате перевода денежных средств в Российской Федерации, Участник вправе принимать от клиентов и выплачивать клиентам денежные средства в российских рублях или долларах США по выбору клиента с учетом ограничений, установленных законодательством Российской Федерации.

3.3.4.2 За пределами Российской Федерации перевод денежных средств может быть выплачен в валюте, отличной от российских рублей и долларов США, с учетом возможностей Платежной Системы в стране выплаты перевода, применимых законодательных ограничений страны выплаты перевода денежных средств и наличия соответствующей валюты в пункте выплаты перевода денежных средств. Курс, по которому валюта отправления пересчитывается в валюту выплаты перевода денежных средств, выбранную отправителем, а также сумма в валюте выплаты сообщаются отправителю перевода денежных средств при отправлении соответствующего перевода и указываются в ПОПДС.

3.3.4.3 В случаях, специально предусмотренных законодательством страны выплаты (включая обязательные к исполнению распоряжения и приказы центральных и (или) национальных банков страны выплаты), при выплате в стране назначения перевод денежных средств может быть принудительно сконвертирован в иную валюту, отличную от валюты, указанной отправителем перевода денежных средств в Российской Федерации, по курсу выплачивающей организации или по курсу центрального банка (национального банка) страны выплаты, установленному на дату выплаты.

3.3.5 Порядок приема денежных средств при осуществлении перевода денежных средств

3.3.5.1 При отправлении перевода денежных средств через Платежную Систему отправитель должен представить Участнику ПОПДС.

3.3.5.2 ПОПДС может быть составлено:

а) отправителем и Участником (его Агентом) на бумажном носителе на бланке по форме, установленной Оператором;

б) Участником по инструкции отправителя путем заполнения сотрудником Участника (сотрудником его Агента) электронной формы в программном обеспечении Платежной Системе с дальнейшей печатью заполненного ПОПДС;

в) отправителем самостоятельно без участия сотрудников Участника (сотрудников Агента) в автоматическом режиме с помощью программных или программно-аппаратных средств Участника (его Агента), позволяющих обеспечивать клиентам Участника доступ к Услугам без непосредственного участия сотрудников Участников (их Агентов).

При составлении ПОПДС с участием сотрудников Участника (его Агента) ПОПДС подписывается отправителем и уполномоченным сотрудником Участника (его Агента) и скрепляется оттиском печати или штампа Участника (его Агента). Наличие подписи отправителя подтверждает

согласие отправителя с Условиями оказания Услуги.

При составлении ПОПДС без участия сотрудников Участника (его Агента) ПОПДС подтверждается отправителем электронной подписью, аналогом собственноручной подписи, кодами, паролями или иным образом, позволяющим подтвердить волеизъявление отправителя и согласие отправителя с Условиями оказания Услуги.

3.3.5.3 ПОПДС содержит:

а) полное ФИО отправителя;

б) данные Документа, удостоверяющего личность отправителя;

в) контактную информацию отправителя;

г) полные имя и фамилию получателя (или наименование организации - получателя, если получателем является юридическое лицо);

д) страну назначения;

е) сумму и валюту перевода, Плату за перевод;

ж) сумму и валюту выплаты перевода, обменный курс.

ПОПДС может содержать дополнительную информацию и реквизиты, обусловленные конкретным видом Услуги или требованиями законодательства.

3.3.5.4 В случае если ПОПДС оформляется отправителем самостоятельно, без участия сотрудников Участника (сотрудников Агента), в автоматическом режиме с помощью программных или программно-технических средств Участника (его Агента), позволяющих обеспечивать клиентам Участника доступ к Услугам без непосредственного участия сотрудников Участников (их Агентов), с последующей возможностью печати ПОПДС на бумажном носителе, такое распечатанное ПОПДС может не содержать отдельные сведения, указанные в п. 3.3.5.3 настоящих Правил.

3.3.5.5 ПОПДС считается принятым к исполнению, если содержит КНДП.

3.3.5.6 Форма ПОПДС может меняться в зависимости от программного обеспечения, используемого Участником (или его Агентом). ПОПДС не содержит данные Документа, удостоверяющего личность получателя, или тип такого документа получателя.

3.3.5.7 Отправление переводов денежных средств, в том числе заполнение ПОПДС, осуществляется с учетом особенностей видов Услуг, указанных в настоящих Правилах.

3.3.5.8 КНДП присваивается переводу денежных средств только после получения Участником (или его Агентом) суммы перевода денежных средств и Платы за перевод в полном объеме в наличной форме или после списания Участником в полном объеме соответствующих сумм с банковского счета отправителя, или после уменьшения доступного баланса счета банковской карты отправителя. Участник несет ответственность за принятие Участником (его Агентом) денежных средств от отправителя, включая Плату за перевод, в полном объеме. Плата за перевод в случае ее взимания взимается Участником с отправителя в полном объеме в валюте отправления перевода денежных средств. В Платежной Системе не допускается принятие Участником от отправителя части наличных денежных средств и части денежных средств в безналичной форме (путем списания денежных средств со счета клиента), в том числе Платы за перевод, в рамках одного перевода денежных средств. Форма и валюта предоставления денежных средств Участнику для целей осуществления перевода денежных средств определяется отправителем с учетом ограничений законодательства Российской Федерации, положений настоящих Правил, а также способов предоставления Участником доступа клиента к Услугам, применяемых Участником.

3.3.5.9 Участник или действующий от его имени Агент осуществляет идентификацию (упрощенную идентификацию) отправителя в соответствии с требованиями законодательства Российской Федерации в области ПОД/ФТ/ФРОМУ. Вне зависимости от вида или суммы Услуги Участник или действующий от его имени Агент имеет право потребовать от отправителя предъявить оригинал Документа, удостоверяющего личность. В случае если отправитель не имеет возможности предъявить оригинал Документа, удостоверяющего личность отправителя, Участник или действующий от его имени Агент может отказаться принять у отправителя ПОПДС. Перечень документов, которые могут быть представлены в целях удостоверения личности при осуществлении идентификации (упрощенной идентификации), определяется в соответствии с требованиями законодательства

Российской Федерации.

3.3.5.10 Ограничения по сумме перевода

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

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

Оператор обеспечивает установление Участнику максимальной суммы отправления одного перевода денежных средств (постоянный трансакционный лимит) и устанавливает Участнику максимальную сумму отправлений переводов денежных средств в течение одного операционного дня (постоянный дневной лимит) в Платежной Системе. В целях обеспечения контроля рисков в Платежной Системе постоянный трансакционный лимит и постоянный дневной лимит устанавливаются и изменяются Оператором в одностороннем порядке. Постоянный трансакционный лимит и постоянный дневной лимит могут устанавливаться на все Отделения, на каждое Отделение в отдельности или на группу Отделений. Аналогичный порядок установления лимитов применяется для Интернет-банка и Терминалов самообслуживания.

3.3.6 Правила выдачи денежных средств при осуществлении переводов денежных средств

3.3.6.1 При выплате перевода денежных средств через Платежную Систему получатель должен представить Участнику ПОВДС.

3.3.6.2 ПОВДС может быть составлено:

а) получателем и Участником (его Агентом) на бумажном носителе на бланке по форме, установленной Оператором;

б) Участником по инструкции получателя путем заполнения сотрудником Участника (сотрудником Агента) электронной формы в программном обеспечении Платежной Системы с дальнейшей печатью заполненного ПОВДС;

в) получателем самостоятельно без участия сотрудников Участника (сотрудников Агента) в автоматическом режиме с помощью программных или программно-аппаратных средств Участника (его Агента), позволяющих обеспечивать клиентам Участника доступ к Услугам без непосредственного участия сотрудников Участников (их Агентов).

При составлении ПОВДС с участием сотрудников Участника (Агента) ПОВДС подписывается получателем и уполномоченным сотрудником Участника (Агента) и скрепляется оттиском печати или штампа Участника (Агента). Наличие подписи получателя подтверждает согласие получателя с Условиями оказания Услуги.

При составлении ПОВДС без участия сотрудников Участника (Агента) ПОВДС подтверждается получателем электронной подписью, аналогом собственноручной подписи, кодами, паролями или иным образом, позволяющим подтвердить волеизъявление получателя и согласие получателя с Условиями оказания Услуги.

3.3.6.3 ПОВДС содержит:

а) полные имя и фамилию получателя;

б) полные имя и фамилию отправителя;

в) страну отправления перевода;

г) сумму к выплате;

д) КНДП.

ПОВДС может содержать дополнительную информацию и реквизиты, обусловленные конкретным видом Услуги или требованиями законодательства.

При составлении ПОВДС через Терминалы самообслуживания, которые не обеспечивают получателю возможность внести полные имя и фамилию отправителя, Участник (Агент) вправе принять такое ПОВДС без указания имени и фамилии отправителя перевода денежных средств, при одновременном соблюдении следующих условий:

- получатель идентифицирован Участником в качестве получателя перевода денежных средств;
- получатель правильно указал страну отправления перевода, сумму к выплате (+/- 10%) и КНДП.

3.3.6.4 Участник или Агент от имени Участника проводит идентификацию получателя во всех случаях вне зависимости от суммы перевода денежных средств. Идентификация получателя осуществляется Участником по правилам идентификации страны отправителя перевода денежных средств.

3.3.6.5 Форма и валюта выдачи денежных средств Участником получателю определяются получателем с учетом ограничений, установленных законодательством Российской Федерации и законодательством страны назначения перевода денежных средств, а также с учетом положений настоящих Правил и способов предоставления Участником доступа своим клиентам к Услугам. В Платежной Системе не допускается выдача Участником получателю части наличных денежных средств и части денежных средств в безналичной форме в рамках одного перевода денежных средств.

3.3.6.6 Переводы денежных средств, поступившие в Российскую Федерацию, выплачиваются на территории Российской Федерации получателю, который:

- предоставляет ПОВДС (с обязательным указанием КНДП);
- предъявляет Документ, удостоверяющий личность, содержащий имя и фамилию получателя, соответствующие имени и фамилии, указанными отправителем при отправлении выплачиваемого перевода денежных средств.

Перед осуществлением выплаты перевода денежных средств получателю Участник, Агент осуществляют проверку имени, отчества (при наличии) и фамилии получателя, указанных в Документе, удостоверяющем личность, на предмет соответствия имени, отчества (при наличии) и фамилии получателя, указанными отправителем при отправлении перевода денежных средств. Участник, Агент не проводят никаких дополнительных проверочных мероприятий в отношении Документа, удостоверяющего личность получателя. Участник, Агент убеждаются в подлинности Документа, удостоверяющего личность, исключительно методом обычного визуального осмотра и не обязаны проводить экспертизу в отношении подлинности Документа, удостоверяющего личность, с помощью специальных экспертных методов и оборудования.

Услуга оказана надлежащим образом в том случае, если перевод денежных средств выдан получателю, личность которого установлена в порядке, предусмотренном законодательством страны назначения перевода денежных средств, имя, отчество(при наличии) и фамилия которого соответствуют имени, отчеству(при наличии) и фамилии получателя, указанными отправителем при отправлении перевода денежных средств, и при условии предоставления получателем ПОВДС с указанием имени, отчества (при наличии) и фамилии отправителя перевода денежных средств (за исключением ПОВДС, предоставляемого в электронном виде через Терминалы самообслуживания), страны отправления перевода денежных средств, имени получателя и КНДП.

При возникновении спорных ситуаций факт надлежащего оказания Услуги в соответствии с поручением отправителя первично считается установленным в случае предоставления отправителю в установленном Условиями оказания Услуги порядке выписки, подготовленной Оператором и содержащей информацию о выплате перевода денежных средств, в том числе имя, отчество(при наличии) и фамилию получателя, страну назначения, наименование организации, осуществившей выплату перевода денежных средств, адрес соответствующей организации, сумму перевода денежных средств, дату выплаты и КНДП. В случае наличия каких-либо сомнений у отправителя или получателя перевода, факт надлежащего оказания Услуги дополнительно подтверждается, организацией, осуществившей выплату соответствующего перевода, путем предоставления Оператору документов (их копий), подтверждающих выплату перевода и позволяющих установить лицо, получившее перевод,

сумму и валюту перевода, дату, место и время выплаты перевода.

3.3.6.7 В случае необходимости получения дополнительных документов и информации от отправителей и (или) получателей может потребоваться предоставление дополнительных документов и информации в адрес Системы, Участников или Партнеров, что может приводить к задержке выплаты перевода денежных средств. Данное требование распространяется на все Услуги.

Сроки предоставления любой Услуги могут быть увеличены, в предоставлении любой Услуги может быть отказано, а отправленный перевод денежных средств может быть заблокирован без каких-либо уведомлений в случаях, предусмотренных нормами законодательства Российской Федерации и законодательства страны выплаты перевода.

3.3.7 Внесение изменений в перевод денежных средств. Аннулирование перевода денежных средств

3.3.7.1 Отправитель имеет право вносить изменения в перевод денежных средств исключительно в отношении переводов денежных средств в пользу физических лиц и исключительно в отношении ФИО получателя, а также в отношении страны назначения перевода в том случае, если Плата за перевод, внесенная отправителем при отправлении соответствующего перевода, равна Плате за перевод, установленной для перевода на такую же сумму в новую страну назначения. Внесение изменений возможно только до момента выплаты соответствующего перевода получателю. Для внесения изменений в отправленный перевод денежных средств отправитель имеет право обратиться к любому Участнику с соответствующим заявлением на внесение изменений.

3.3.7.2 Аннулирование перевода денежных средств в пользу физического лица осуществляется по правилам внесения изменений в перевод денежных средств. При аннулировании перевода денежных средств в пользу физического лица дополнительная плата с отправителя не взимается.

3.3.8 Порядок предъявления и рассмотрения претензий клиентов

3.3.8.1 Порядок предъявления и рассмотрения претензий клиентов о ненадлежащей выплате

3.3.8.1.1 Претензии клиентов о ненадлежащей выплате принимаются Участниками (их Агентами) в соответствии с процедурой, установленной в Условиях оказания Услуги.

3.3.8.1.2 После получения Участником (его Агентом) пакета документов, предусмотренных Условиями оказания Услуги для подачи претензии о ненадлежащей выплате, Участник направляет соответствующий пакет Оператору для проведения расследования.

3.3.8.1.3 Оператор проводит расследование и направляет Участнику заключение не позднее чем через 20 (двадцать) календарных дней с даты получения пакета документов от Участника.

3.3.8.1.4 В случае, если в результате расследования Оператор установит, что отправленный перевод денежных средств выплачен ненадлежащему получателю или выплачен не в полном объеме, Участник возвратит отправителю сумму перевода денежных средств вместе с Платой за перевод. При этом сумма перевода денежных средств и Плата за перевод выплачиваются:

а) за счет средств Участника, осуществившего отправление перевода денежных средств в случае, если при отправлении перевода денежных средств Участником (его Агентом) были нарушены настоящие Правила;

б) за счет средств Участника, осуществившего выплату перевода денежных средств в случае, если при выплате перевода денежных средств Участником (его Агентом) были нарушены настоящие Правила;

в) за счет средств Оператора и/или Оператора УПИ и/или Партнера в случае, если ненадлежащая выплата перевода денежных средств была вызвана нарушением Оператором и/или Оператором Услуг Платежной Инфраструктуры настоящих Правил, а также при наличии нарушений на стороне Партнера, осуществившего выплату перевода денежных средств за пределами Российской Федерации.

3.3.8.1.5 Оператор или Участник имеют право компенсировать отправителю за свой счет иные расходы клиента, вызванные ненадлежащей выплатой перевода денежных средств.

3.3.8.1.6 В случае если в результате расследования Оператор установит, что отправленный перевод денежных средств выплачен надлежащему получателю и в полном объеме, Оператор подготовит и направит Участнику выписку о надлежащей выплате перевода денежных средств, содержащую информацию о выплате перевода денежных средств, в том числе имя, отчество(при наличии) и фамилию получателя, страну назначения, наименование организации, осуществившей выплату перевода денежных средств, адрес пункта выплаты соответствующей организации, сумму перевода денежных средств, дату выплаты и КНДП. Предоставление такой выписки Оператором Участнику является для Участника основанием для отказа в удовлетворении претензии о ненадлежащей выплате. После получения соответствующей выписки от Оператора, подтверждающей надлежащую выплату перевода денежных средств, Участник вправе самостоятельно и за счет собственных средств Участника осуществить возврат перевода денежных средств отправителю вместе с Платой за перевод (или без возмещения Платы за перевод по усмотрению Участника).

3.3.8.2 Порядок предъявления и рассмотрения иных претензий клиентов

3.3.8.2.1 Иные претензии клиентов, не связанные с ненадлежащей выплатой переводов денежных средств, предъявляются клиентами в соответствии с Условиями оказания Услуги.

3.3.8.2.2 Участник вправе самостоятельно предоставлять ответы своим клиентам на их претензии, не связанные с ненадлежащей выплатой переводов денежных средств, поступившие Участнику или его Агенту, или передавать их на рассмотрение Оператору.

3.3.8.2.3 При поступлении претензии Оператору от клиента Участника, направленной таким клиентом непосредственно Оператору или переданной Участником, Оператор вправе запрашивать у Участника документы и информацию, необходимые для ответа на соответствующую претензию.

3.3.8.2.4 В случае, если в результате рассмотрения претензии Оператор выявит нарушения Участником (его Агентом) настоящих Правил, Оператор вправе применять к Участнику санкции, предусмотренные настоящими Правилами.

3.4 Порядок оплаты Услуги

3.4.1 Плата за перевод взимается Участником (его Агентом) с отправителя перевода денежных средств. Такая Плата за перевод фиксируется и отображается в информационном окне программного обеспечения Платежной Системы и доступна для просмотра Участником (его Агентом) в момент осуществления операции по отправлению перевода денежных средств. В случае отправления перевода денежных средств в пользу юридического лица Плата за перевод может взиматься с получателя перевода денежных средств. В случае если Плата за перевод взимается с получателя перевода – юридического лица, такая Плата за перевод фиксируется и отображается в информационном окне программного обеспечения Платежной Системы и доступна для просмотра Участником в момент осуществления операции по отправлению перевода денежных средств. В случае взимания Платы за перевод с получателя перевода – юридического лица Плата за перевод может взиматься с отправителя перевода денежных средств исключительно, если это указано в информационном окне программного обеспечения Платежной Системы. Плата за перевод не взимается с получателя денежных средств – физического лица.

3.4.2 Плата за перевод взимается Участником (его Агентом) с отправителя перевода денежных средств в валюте отправления перевода денежных средств. В случае взимания Платы за перевод с получателя денежных средств такая Плата за перевод взимается в валюте выплаты перевода денежных средств.

3.4.3 Плата за перевод, взимаемая с отправителя перевода денежных средств, взимается Участником:

а) наличными в случае принятия суммы перевода денежных средств в наличной форме;

б) путем списания денежных средств со счета отправителя перевода денежных средств в

случае принятия суммы перевода денежных средств путем списания денежных средств со счета отправителя перевода денежных средств.

В Платежной Системе не допускается полный или частичный прием денежных средств Участником (его Агентом) от отправителя в оплату Платы за перевод в форме и в валюте, отличной от той, в которой Участником (его Агентом) принята сумма такого перевода денежных средств.

3.5 Размер платы за перевод

3.5.1 Плата за перевод, взимаемая Участниками (Агентами) с отправителей или получателей денежных средств, устанавливается Оператором и отображается в информационном окне программного обеспечения Платежной Системы и доступна для просмотра Участником (Агентом) в момент осуществления операции по отправлению перевода денежных средств. Плата за перевод в отношении Услуг, оказываемых Участниками своим клиентам-отправителям переводов денежных средств, устанавливается в соответствии с Приложением №5 к настоящим Правилам. Участник уведомляет своих клиентов о размере Платы за перевод путем размещения информации о размере Платы за перевод в Отделениях, Интернет-банке, Терминалах самообслуживания, а также на сайте Участника (Агента).

3.5.2 Участник обязуется обеспечить ознакомление своих клиентов с размером Платы за перевод до момента оказания им Услуги.

3.5.3 Участник обязуется не взимать с отправителей и/или получателей денежных средств никаких дополнительных плат, за исключением Платы за перевод.

3.6 Программа лояльности и проведение маркетинговых (стимулирующих) акций

3.6.1 Оператор вправе организовывать и проводить программы лояльности для клиентов, пользующихся Услугами.

3.6.2 Оператор вправе устанавливать правила программ лояльности, организованных Оператором.

3.6.3 Правила программ лояльности размещаются Оператором на сайте www.omnypay.ru.

3.6.4 Оператор вправе проводить различные маркетинговые (стимулирующие) акции и другие маркетинговые мероприятия, связанные с установлением на определенный срок специального размера Платы за перевод в целях продвижения Услуг, стимулирования Участников и их клиентов (далее «Маркетинговые акции»). Маркетинговые акции могут распространяться на определённую территорию, отдельных Участников, отдельные Услуги или отдельные способы предоставления доступа клиентам Участников к Услугам. Оператор имеет право в любой момент времени отменить или изменить условия проводимых Маркетинговых акций, а также продлить срок действия указанных Маркетинговых акций неограниченное количество раз. Информация о проводимых акциях доводится до сведения вовлеченных в Маркетинговую акцию Участников заблаговременно путем направления соответствующей информации на адреса электронной почты Участников. Информация о Маркетинговых акциях может публиковаться Оператором на сайте www.omnypay.ru.

3.6.5 Без предварительного письменного согласия Оператора Участники не имеют права предоставлять клиентам какие-либо скидки на Услуги, за исключением скидок, предусмотренных программами лояльности или Маркетинговыми акциями, организованными Оператором.

3.7 Осуществление Участником идентификации клиентов в пользу других Участников

3.7.1 При оказании клиенту Услуги Участник соглашается осуществлять идентификацию такого клиента в полном соответствии с Федеральным законом от 07.08.2001 № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» для целей оказания Услуги данному клиенту, а также для целей оказания Услуги другими Участниками в случаях, предусмотренных в п. 3.7.4 настоящих Правил (далее «Идентификация в пользу других Участников»).

3.7.2 В рамках осуществления Идентификации в пользу других Участников Участник передает Оператору идентификационные данные клиента, полученные Участником от клиента при оказании Услуги, для дальнейшего использования таких данных другими Участниками.

3.7.3 Оператор создает и обеспечивает поддержку базы данных, содержащую данные идентифицированных клиентов, полученные Оператором от Участников в рамках Идентификации в пользу других Участников (далее «База данных идентифицированных клиентов») и будет предоставлять данные из Базы данных идентифицированных клиентов Участникам для целей оказания Участниками Услуги своим клиентам. Оператор должен обеспечить обновление данных, содержащихся в Базе данных идентифицированных клиентов, на регулярной основе, но не реже одного раза в год.

3.7.4 Данные, содержащиеся в Базе данных идентифицированных клиентов, предоставляются Оператором Участникам для целей оказания Участниками Услуг в Терминалах самообслуживания Участников или их Агентов при условии наличия технологической возможности передачи таких данных Оператором Участнику в режиме реального времени и обеспечения возможности подтверждения клиентом таких данных в момент оказания Услуги путем введения клиентом разового кода или пароля.

Глава 4. Участники

4.1 Виды и критерии участия в Платежной Системе

4.1.1 Платежная Система предусматривает исключительно прямое участие. Наличие косвенных участников в Платежной Системе не предусматривается.

4.1.2 Участники осуществляют расчеты в рамках Платежной Системы непосредственно через РЦ в соответствии с настоящими Правилами (а в случае привлечения сторонних РЦ в соответствии с настоящим Правилами и договорами с такими привлеченными РЦ).

4.1.3. Участником Платежной Системы может стать организация, соответствующая одновременно следующим критериям:

4.1.3.1. Общие критерии:

- организация является кредитной организацией; - в соответствии с лицензией организация уполномочена осуществлять переводы денежных средств без открытия счета.

4.1.3.2. Критерии, касающиеся финансового состояния:

- у организации отсутствует просроченная задолженность по платежам в бюджет в соответствии с законодательством Российской Федерации;

- у организации отсутствуют судебные иски и/или судебные решения с размером обязательств равным и более 10% от величины его чистых активов.

4.1.3.2. Критерии, касающиеся технологического обеспечения:

- - техническая инфраструктура организации соответствует обязательным требованиям законодательства и требованиями нормативных актов Банка России, установленным для операторов по переводу денежных средств, осуществляющих переводы денежных средств;

- организация подтверждает готовность выполнять требования Главы 8 Правил в части требований к Участникам.

4.1.3.3. Иные критерии:

- наличие в структуре организации специального подразделения или уполномоченного лица для взаимодействия с Субъектами Системы;

- готовность предоставления организацией Оператору периодических отчетов о работе в Системе.

4.2 Порядок присоединения Участников к Платежной Системе

4.2.1 Операторы по переводу денежных средств – российские кредитные организации, намеревающиеся стать Участниками (далее «Заявитель»), направляют Оператору заявление по форме Приложения № 1 к настоящим Правилам. Направление заявления не является подтверждением присоединения Заявителя к Правилам.

4.2.2 Вместе с заявлением Заявитель представляет Оператору пакет документов в соответствии с перечнем, утвержденным Оператором. Для привлечения Агентов Заявителя в целях оказания Услуг, Заявитель представляет пакет документов в отношении своих Агентов в соответствии с перечнем, установленным Оператором. Перечень необходимых документов, а также формы документов размещаются Оператором на сайте www.omnypay.ru.

4.2.3 Все документы предоставляются Заявителем Оператору на бумажных носителях и должны быть нотариально удостоверены или заверены подписью уполномоченного лица Заявителя и оттиском печати Заявителя. Все документы также предоставляются Заявителем в электронном виде на адрес электронной почты Оператора, указанный на сайте www.omnypay.ru.

4.2.4 В срок, не превышающий 30 (тридцати) дней после получения Оператором полного пакета документов Заявителя в оригинале, Оператор выносит внутренние заключения Оператора в отношении уровня кредитного риска, правовое заключение, заключение подразделения по ПОД/ФТ и иные заключения в соответствии с внутренними документами Оператора. Указанный тридцатидневный срок может быть продлен Оператором по его усмотрению в случае необходимости проведения дополнительных проверок или получения дополнительной информации от Заявителя. Для целей подготовки соответствующих заключений, Оператор вправе привлекать Операторов УПИ, являющихся кредитными организациями.

4.2.5 В течение 5 (пяти) рабочих дней после вынесения положительных заключений, указанных в п. 4.2.4 выше, Оператор подготавливает и направляет Заявителю оферту, составленную по форме Приложения № 2 к Правилам и содержащую (далее «**Оферта**»):

i. ставку вознаграждения Участника;
ii. перечень Услуг, которые Участник будет оказывать своим клиентам в рамках Платежной Системы;
iii. способ обеспечения доступа Участника к Платежной Системе;
iv. способ(ы) предоставления Участником доступа своим клиентам к Услугам, включая каналы предоставления Услуг Участником;
v. размеры лимитов;
vi. Отчетный период для целей расчетов и пороговые величины задолженности;
vii. размер и порядок расчета гарантийного взноса, перечисляемого Участником в гарантийный фонд Платежной Системы;
viii. информацию о необходимости заключения между Участником и Оператором договоров о выделенном канале связи, об интеграции или защищенном документообороте, а также иных договоров, заключение которых обусловлено способом обеспечения доступа Участника к Платежной Системе;
ix. дополнительные требования к защите информации в соответствии со способом обеспечения доступа Участника к Платежной Системе;
x. срок действия Оферты;
xi. иные условия сотрудничества.

В случае вынесения отрицательных заключений, указанных в п. 4.2.4 выше, Оператор в течение срока, установленного в настоящем п. 4.2.5, направляет Заявителю отказ. Оператор оставляет за собой право не указывать причины отказа.

4.2.6 Оферта направляется Заявителю в двух экземплярах.

4.2.7 После получения Оферты Заявитель заполняет часть Оферты, предназначенную для заполнения Заявителем (далее «Акцепт»), и направляет 1 (один) экземпляр в адрес Оператора. Акцепт является согласием Участника на присоединение к настоящим Правилам. Любой Участник присоединяется к Правилам путем принятия их в целом в соответствии с требованиями части 7 статьи

20 Федерального закона от 27.06.2011 года № 161-ФЗ. В случае, если Акцепт направлен Оператору в пределах срока действия Оферты, Оператор после получения Акцепта направляет Заявителю уведомление о подтверждении даты начала участия Заявителя в Платежной Системе, которое содержит дату начала участия Заявителя в Платежной Системе и номер Участника (далее «Уведомление о начале участия»). Заявитель становится Участником на условиях Оферты и настоящих Правил с даты, указанной в Уведомлении о начале участия.

4.2.8 Участник приступает к осуществлению переводов денежных средств в рамках Платежной Системы после выполнения следующих условий:

а) присвоения Участнику Оператором номера Участника, позволяющего однозначно установить Участника;

б) регистрации не менее одного Отделения, Интернет-банка или Терминала самообслуживания Участника в Платежной Системе;

в) внесения Участником гарантийного взноса в Гарантийный фонд в случае, если условия Оферты предполагают внесение гарантийного взноса Участником;

г) открытия Участником корреспондентских счетов в валютах расчета в РЦ.

4.3. Порядок присвоения Участнику номера Участника, позволяющего однозначно установить Участника в Платежной Системе

4.3.1 После получение Акцепта Оператор присваивает Участнику четырехзначный номер Участника. Цифры номера являются порядковым номером Оферты и могут содержать цифры от 0 до 9. В течение всего срока участия в Платежной Системе за Участником сохраняется номер Участника.

4.3.2 Оператор ведет реестр Участников и учет номеров Участников.

4.4 Обязанности Участника

Участник обязан:

i) соблюдать настоящие Правила в полном объеме;

ii) оказывать Услуги в соответствии с перечнем Услуг, установленным в Оферте;

iii) принимать ПОПДС и ПОВДС, соответствующие требованиям настоящих Правил;

iv) при поступлении ПОВДС, соответствующего требованиям настоящих Правил, осуществлять выплату перевода денежных средств получателю в соответствии с настоящими Правилами, до момента фактического поступления денежных средств Участнику;

v) обеспечить регистрацию Отделений в соответствии с процедурой регистрации Отделений, установленной настоящими Правилами;

vi) использовать собственные или арендованные помещения, необходимое оборудование и назначать персонал в целях осуществления перевода денежных средств в рамках Платежной Системы;

vii) обеспечить полную конфиденциальность в отношении любой информации, связанной с работой Платежной Системы, всеми сотрудниками Участника или его Агента, которые будут непосредственно работать с Платежной Системой, а также сотрудниками Участника, которые по должности смогут иметь доступ к документации и информации в связи с работой в Платежной Системе;

viii) обеспечить каналы связи, необходимые для подключения Участника к Платежной Системе с учетом положений Оферты;

ix) с момента начала работы Участника в Платежной Системе обеспечить комплекс необходимых мер для контроля за тем, чтобы Платежная Система не использовалась клиентами Участника в целях обхода ограничений, установленных законодательством Российской Федерации и органами валютного регулирования, а также с целью легализации (отмывания) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения;

x) с момента начала работы Участника в Платежной Системе обеспечивать обслуживание клиентов специально назначенным Участником персоналом;

xi) при оказании Услуг не взимать с клиентов никаких дополнительных сборов, за исключением прямо предусмотренных настоящими Правилами;

xii) в случае возникновения обстоятельств, временно препятствующих продолжению оказания Услуг в Отделениях или Интернет-банке, в день их возникновения информировать об этом Оператора и ОЦ с указанием сроков временного прекращения и последующего возобновления деятельности. При этом до момента возобновления работы Отделения, Интернет-банка Участник обязуется переадресовывать все телефонные звонки и обращения клиентов относительно Услуг в СПК. При изменении времени работы Отделений, номеров телефонов, факсов, замене ответственных лиц уведомлять Оператора и ОЦ на следующий рабочий день после таких изменений;

xiii) информировать Оператора об изменении фактического местонахождения, наименования Участника, а также о смене единоличного исполнительного органа Участника в течение двух недель после вступления в силу таких изменений. Кроме того, Участник в указанные в настоящем пункте сроки обязуется своевременно уведомлять Оператора о смене почтового адреса, номера факсимильной связи, адресов электронной почты для направления уведомлений и иной информации, связанной с работой Участника в Платежной Системе. Оператор не несет ответственности за несвоевременное уведомление Участника об изменениях настоящих Правил, вызванное неисполнением Участником своих обязательств по уведомлению Оператора о смене почтового адреса, номера факсимильной связи, адресов электронной почты для направления уведомлений;

xiv) размещать снаружи на помещениях Отделений в зоне видимости клиентов, на интернет - сайте Участника (Агентов), в интерфейсе Интернет-банка и Терминалов самообслуживания, информационные материалы об участии Участника в Платежной Системе при условии согласования дизайна таких информационных материалов с Оператором;

xv) включать в информационные материалы Участника, размещенные в Отделениях (в том числе в электронном виде), на интернет-сайте Участника, в Интернет-банке и в Терминалах самообслуживания в обязательном порядке информацию о размере Платы за перевод, Условия оказания Услуги (в том числе в виде гиперссылки) и, по решению Участника, дополнительную информацию об оказании Участником Услуги;

xvi) обеспечить клиентам возможность ознакомления с Условиями оказания Услуги до наступления Безотзывности перевода денежных средств;

xvii) доводить до сведения клиентов условия выплаты и ограничения, действующие в стране назначения перевода денежных средств, отправляемого в рамках Услуги, до момента наступления Безотзывности, перевода денежных средств;

xviii) обеспечить получение согласия клиента с Условиями оказания Услуги до момента наступления Безотзывности перевода денежных средств и по первому требованию Оператора предоставлять Оператору документальное подтверждение такого согласия;

xix) в информацию для клиентов о работе Участника по возможности включать сведения о его деятельности по оказанию Услуг, предварительно согласовав в письменной форме эти сведения с Оператором, строго придерживаться знака обслуживания и логотипа Платежной Системы, не допускать появления сведений, которые могут ввести в заблуждение клиентов или нанести ущерб репутации Платежной Системы;

xx) предварительно согласовывать в письменном виде с Оператором любую информацию, публикуемую Участником, в отношении Оператора или Платежной Системы (включая, но не ограничиваясь, пресс-релизы, рекламу и т.д.);

xxi) перечислять по требованию Оператора гарантийный взнос в гарантийный фонд Платежной Системы в соответствии с положениями Оферты;

xxii) после присвоения номера Участника открыть банковские счета в РЦ для целей расчетов в рамках Платежной Системы по каждой из валют расчета;

xxiii) обеспечить наличие денежных средств на банковских счетах, открытых в РЦ, в сумме, достаточной для расчетов с Оператором по каждой из валют расчета;

xxiv) хранить не менее пяти лет с момента осуществления перевода денежных средств ПОПДС и ПОВДС, принятые Участником (Агентом) по каждому конкретному переводу денежных средств;

xxv) по первому требованию немедленно предоставлять Оператору любую документацию,

касающуюся переводов денежных средств, осуществленных Участником в рамках Платежной Системы;

xxvi) оказывать Оператору полное содействие в реализации любых предусмотренных законодательством мер для защиты информации, составляющей его коммерческую тайну.

xxvii) принимать ПОПДС и ПОВДС, составленные с использованием безбланковой технологии;

xxviii) не вносить никакие изменения в интерфейс, телекоммуникации и алгоритм работы программного обеспечения Платежной Системы, обеспечивающие взаимодействие Участника (Агента) с процессингом Платежной Системы, без предварительного письменного уведомления и согласия Оператора;

xxix) предоставлять по запросу Оператора информацию по применяемым Участником (Агентами) процедурам в области ПОД/ФТ/ФРОМУ в случаях, когда предоставление такой информации не противоречит действующему законодательству Российской Федерации. Предоставление такой информации может осуществляться в письменном виде, в форме электронных сообщений, в устной форме во время встреч, организуемых представителями соответствующих структурных подразделений Участника и Оператора, путем заполнения Участником специальных анкет, направляемых Оператором Участнику, а также иными согласованными между Участником и Оператором способами;

xxx) предоставлять Оператору по его требованию бухгалтерскую отчетность Участника по формам 0409101, 0409123 и 0409135, а также бухгалтерскую отчетность Участника по форме 0409102. Отчетность предоставляется Участником Оператору в течение 3 (трех) рабочих дней после получения Участником соответствующего требования Оператора. Формы отчетности направляются Участником в электронном виде по согласованным с оператором каналам связи;

xxxi) не привлекать третьих лиц к оказанию Услуги (в том числе Агентов) без предварительного письменного согласия Оператора и не заключать с третьими лицами без предварительного письменного согласия какие-либо договоры, связанные с оказанием Участником Услуг;

xxxii) в случае привлечения Агентов в порядке, предусмотренном настоящими Правилами, нести полную ответственность перед Оператором и третьими лицами за любые действия (бездействие) таких Агентов;

xxxiii) в случае привлечения Агентов в порядке, предусмотренном настоящими Правилами, обеспечить исполнение Агентами настоящих Правил;

xxxiv) использовать все установленные законодательством процедуры для обеспечения защиты персональных данных клиентов, а также процедуры, применяемые Оператором, в случае, если применение таких процедур является коммерчески обоснованным;

xxxv) отказать клиенту в отправке или выплате перевода денежных средств, в случае, если клиент Участника отказывается от подписания ПОПДС или ПОВДС, содержащую Условия оказания Услуги;

xxxvi) получать от своих клиентов, обратившихся за выплатой или отправкой переводов денежных средств, прямое выраженное согласие на обработку (включая передачу) персональных данных субъектам Платежной Системы, по форме, установленной Оператором;

xxxvii) внести в процессинг Платежной Системы информацию о согласии клиента в целях обеспечения ненарушения волеизъявления клиента;

xxxviii) получить прямое выраженное письменное согласие сотрудников Участника на передачу их персональных данных Оператору и Операторам УПИ для целей исполнения Участником своих обязательств предусмотренных настоящими Правилами, направления поздравлений и подарков, организации поездок в рамках программ мотивации и предоставлять по требованию Оператора копии таких согласий;

xxxix) обеспечить сохранность и защиту всех данных клиентов, включая подписанные ПОПДС и ПОВДС, и предпринимать все меры, предусмотренные законодательством, для защиты данных от несанкционированного доступа, а также от обработки и использования персональных данных клиентов сотрудниками Участника или третьими лицами в целях, противоречащих целям обработки

персональных данных, установленных в соответствии с законодательством или настоящими Правилами;

xl) использовать процедуры для выявления утраты или несанкционированного раскрытия персональных данных. Участник незамедлительно уведомит Оператора о любых случаях несанкционированного раскрытия персональных данных или несанкционированного доступа к персональным данным и будет сотрудничать с Оператором по вопросам урегулирования последствий такого раскрытия или доступа;

xli) обеспечить защищенную передачу персональных данных при любой передаче персональных данных;

xlii) после прекращения участия в Платежной Системе стереть или уничтожить без возможности восстановления персональные данные, полученные Участником в рамках участия в Платежной Системе, в соответствии с требованиями законодательства Российской Федерации, за исключением случаев, когда продолжение обработки персональных данных требуется в соответствии с законодательством Российской Федерации;

xliii) обеспечить реализацию процессов выявления и идентификации риска информационной безопасности в Платежной Системе в отношении объектов информационной инфраструктуры Участника;

xliv) обеспечить выявление и анализ Участником риска информационной безопасности в Платежной Системе;

xlv) нести иные обязательства, прямо предусмотренные законодательством Российской Федерации и настоящими Правилами.

4.5 Права Участника

Участник имеет право:

i) взимать с отправителей переводов денежных средств Плату за перевод;

ii) требовать от Оператора уплаты вознаграждения Участника за осуществление отправления и выплаты перевода;

iii) самостоятельно распоряжаться денежными средствами, находящимися на счетах Участника в РЦ, в соответствии с условиями договоров банковского счета, заключенных между Участником и РЦ;

iv) требовать от Оператора возврата гарантийного взноса, перечисленного Участником в гарантийный фонд Платежной Системы;

v) в течение рабочего времени СПК и Оператора обращаться в СПК или непосредственно к Оператору по вопросам, связанным с оказанием Участником Услуг;

vi) направлять Оператору запросы в отношении жалоб и претензий клиентов, поступивших в адрес Участника;

vii) в случаях, предусмотренных настоящими Правилами, получать выписки из процессинга Платежной Системы в отношении переводов денежных средств, отправленных Участником;

viii) направлять Оператору заявления на регистрацию Отделений, Интернет-банка и Терминалов самообслуживания для работы в Платежной Системе в порядке, установленном Оператором;

ix) получать от Оператора доступ к программному обеспечению Платежной Системы, необходимый для взаимодействия с процессингом Платежной Системы, в соответствии с положениями Оферты;

x) требовать от Оператора надлежащего исполнения обязательств Оператора;

xi) запрашивать у Оператора размер Платы за перевод и информационные материалы;

xii) самостоятельно определять конкретные способы и методы защиты информации на стороне Участника при осуществлении переводов денежных средств через Платежную Систему с учетом требований, установленных в законодательстве Российской Федерации и настоящих Правилах;

xiii) пользоваться иными правами, предусмотренными законодательством Российской Федерации и настоящими Правилами.

4.6 Регистрация Отделений и Интернет-банка

4.6.1 Для целей осуществления переводов денежных средств Участник регистрирует свои Отделения и (или) Интернет-банк и (или) Терминалы самообслуживания в Платежной Системе в соответствии с настоящими Правилами. В каждом из таких Отделений и (или) Интернет-банке могут быть зарегистрированы один и более терминалы для ввода данных в Платежную Систему.

4.6.2 Для регистрации Отделения и/или Интернет-банка и/или Терминал самообслуживания Участника в Платежной Системе Участник направляет в адрес ОЦ заявку по форме, установленной Оператором. Между ОЦ и Участником предусматривается возможность направления заявки в электронной форме, что определяется положениями Оферты. Оператор и/или ОЦ оставляет за собой право заблокировать аппаратными методами доступ Отделения и/или Интернет-банка и/или Терминала самообслуживания к Платежной Системе в случае, если через такое Отделение и/или Интернет-банк и/или Терминал самообслуживания не было совершено ни одного перевода денежных средств (выплаты или отправления) в течение 12 (двенадцати) месяцев с даты регистрации Отделения и/или Интернет-банка и/или Терминала самообслуживания. При этом заявка Участника на регистрацию признается аннулированной. Оператор или ОЦ могут уведомить сотрудника Участника, ответственного за работу Участника в Платежной Системе, о таком решении.

4.6.3 Внесение изменений в регистрационные данные Отделения и/или Интернет-банка осуществляется Участником по процедуре регистрации Отделений.

4.7 Порядок привлечения Агентов

4.7.1 Участники с предварительного письменного согласия Оператора вправе самостоятельно привлекать Агентов. При этом, Участники вправе привлекать своих Агентов для целей оказания Услуги только при условии предварительного подтверждения Оператором соответствия привлекаемых Агентов требованиям Правил Платежной Системы.

4.7.2 Привлечение Участником Агента осуществляется в следующем порядке:

4.7.2.1 До привлечения Агента для работы в Платежной Системе, Участник предоставляет Оператору следующую информацию:

- Анкету Агента, по форме, установленной Оператором с приложением документов, их копий, указанных в анкете;

- справку в свободной форме, которая должна включать следующую информацию:

- кол-во и георграфия точек обслуживания, в которых планируется осуществление Денежных Переводов;
- планируемый набор операций;
- описание процедуры идентификации клиентов и подтверждение Участником соответствие процедуры идентификации клиентов требованиям законодательства Российской Федерации;
- описание инструментов контроля, применяемых Участником в отношении деятельности Агента;
- подтверждение Участника о соблюдении Участником требований по привлечению банковских платежных агентов при привлечении Агента, установленных законодательством;
- информацию о технических и организационных способах защиты информации, применяемых Агентом (для целей осуществления деятельности в рамках Платежной Системы);
- гарантии и заверения Участника в отношении принятия на себя ответственности за деятельность Агента;
- иную информацию по усмотрению Участника.

4.7.2.2 Оператор рассматривает информацию, предоставленную Участником, и имеет право запросить дополнительную информацию в отношении Агента у Участника.

4.7.2.3. Оператор имеет право отказать Участнику в привлечении Агента в следующих случаях:

- на основании анализа информации, предоставленной Участником, Оператор обоснованно полагает, что привлечение Агента создает или может создать финансовый, операционный, юридический или репутационный риск для Оператора, Операторов УПИ или Платежной Системы; или
- привлечение Агента создает угрозу нарушения БФПС;
- Участник не предоставил дополнительную информацию, запрошенную Оператором.

4.7.2.4. При отсутствии оснований, указанных в п. 4.7.2.3. выше, Оператора предоставляет Участнику согласие на привлечение Агента в течение 30 (тридцати) календарных дней после предоставление Участником Оператору информации, указанной в п. 4.7.2.1. Согласие действует в течение шести месяцев после даты его предоставления.

4.7.2.5. После получения согласия Оператора Участник регистрирует точки Агента для работы в Платежной Системе в качестве Отделений Участника.

4.8 Инструктивные материалы

4.8.1 Детальное описание каждого вида Услуг, порядок действий сотрудников Участника (его Агента) при предоставлении отдельных видов Услуг, рекомендации по обслуживанию клиентов, инструкции по работе с программным обеспечением Платежной Системы , инструкции по взаимодействию с Операторами УПИ, инструкции по расчетам и иные инструкции, связанные с работой с Платежной Системой, предоставляются Участнику при присоединении к настоящим Правилам в зависимости от перечня Услуг, предоставляемых Участником, способов предоставления доступа к Услугам, реализованных у Участника, а также иных особенностей взаимодействия Участника и Оператора или Оператора Услуг Платежной Инфраструктуры (далее «**Инструктивные материалы**»).

4.8.2 Инструктивные материалы являются документами, носящими рекомендательный характер и позволяющими построить процессы работы Участника в Платежной Системе. Инструктивные материалы не являются частью настоящих Правил.

4.8.3 Все Инструктивные материалы содержат сведения и информацию, составляющие коммерческую тайну Оператора. Участник, получивший Инструктивные материалы, обеспечит конфиденциальность содержания Инструктивных материалов и не будет передавать такие Инструктивные материалы третьим лицам, за исключением случаев, предусмотренных законодательством Российской Федерации. В случае прекращения участия Участника в Платежной Системе Участник вернет все копии Инструктивных материалов Оператору или за свой счет уничтожит их и подтвердит Оператору факт уничтожения Инструктивных материалов.

4.9 Срок присоединения Участника к Правилам

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

4.10 Приостановление и прекращение участия в Платежной Системе

4.10.1 Приостановление участия в Платежной Системе.

4.10.1.1 Под приостановлением участия в Платежной Системе понимается блокирование

доступа некоторых Отделений и (или) Интернет-банка Участника к Платежной Системе и/или блокирование возможности некоторых Отделений и (или) Интернет-банка и(или) Терминалов самообслуживания Участника осуществлять отдельные виды Услуг по заявлению Участника или по решению Оператора в случаях, предусмотренных в п. 4.10.1.3. настоящих Правил. При этом Участник продолжит соблюдать настоящие Правила, за исключением положений настоящих Правил, продолжение исполнения которых невозможно в связи с блокированием доступа всех или некоторых Отделений и (или) Интернет-банка и(или) Терминалов самообслуживания Участника к Платежной Системе.

4.10.1.2 Участие в Платежной Системе может быть приостановлено по заявлению Участника на срок не более одного месяца с даты получения Оператором соответствующего заявления в случае, если Участник по техническим причинам не может обеспечить оказание Услуги в соответствии с настоящими Правилами. Участие такого Участника возобновляется в Платежной Системе с момента получения Оператором уведомления Участника о возобновлении участия, не позднее одного месяца с даты получения Оператором заявления о приостановлении участия.

4.10.1.3 Участие в Платежной Системе может быть приостановлено по решению Оператора:

- на срок до трех месяцев в случае, если Оператор обоснованно полагает, что продолжение оказания Услуг Участником во всех или некоторых Отделениях и (или) Интернет-банке может противоречить действующему законодательству Российской Федерации, включая, но не ограничиваясь законодательством о ПОД/ФТ/ФРОМУ;

- вплоть до устранения соответствующего нарушения, в случае нарушения Участником настоящих Правил или нарушения Участником требований по ПОД/ФТ/ФРОМУ, установленных настоящими Правилами, включая требования пункта 10.1.4 Правил.;

- вплоть до погашения Участником задолженности перед Оператором в случае наличия непогашенной задолженности Участника перед Оператором;

- на срок, определяемый Оператором в случае, если:

а) единовременно продано, передано или отчуждено более 10% (десяти процентов) от балансовой стоимости активов Участника;

или

б) происходят существенные изменения в структуре контроля над Участником;

или

в) Участник без предварительного письменного согласия Оператора предпринимает какие-либо действия, направленные на частичную или полную передачу своих прав и обязательств в соответствии с настоящими Правилами; или

г) в иных случаях, предусмотренных настоящими Правилами и законодательством Российской Федерации.

В любом из указанных выше случаев участие в Платежной Системе немедленно приостанавливается Оператором с последующим письменным уведомлением Участника о сроках и порядке возобновления участия такого Участника в Платежной Системе.

4.10.2 Прекращение участия в Платежной Системе

4.10.2.1 Участие Участника в Платежной Системе может быть прекращено по письменному соглашению между Участником и Оператором.

4.10.2.2 Участие Участника может быть прекращено по заявлению Участника в порядке, предусмотренном п. 4.9.1 настоящих Правил.

4.10.2.3 Участие Участника в Платежной Системе прекращается автоматически в случае:

а) отзыва у Участника Банком России лицензии, в соответствии с которой Участник осуществляет переводы денежных средств; или

б) прекращения деятельности Платежной Системы.

4.10.2.4 Уведомления, направляемые в соответствии с настоящим п. 4.10.2, должны быть оформлены в письменном виде и подписаны лицами, которые имеют право подписывать соответствующие документы на основании устава, доверенности или иного документа,

подтверждающего их полномочия. Такие уведомления должны быть выполнены на фирменном бланке и скреплены оттиском печати организации – отправителя уведомления.

4.10.2.5. Прекращение участия Участника в Платежной Системе влечет прекращение оказания услуг платежной инфраструктуры Участнику и его клиентам.

4.11 Последствия прекращения участия

4.11.1 Не позднее 2 (двух) рабочих дней после прекращения участия Участник и Оператор осуществляют взаиморасчеты.

4.11.2 В случае недостаточности денежных средств на счетах Участника, открытых в РЦ, обязательства Участника исполняются за счет средств гарантийного взноса, перечисленных Участником в гарантийный фонд Платежной Системы. Неизрасходованный остаток гарантийного взноса перечисляется Оператором на счет, указанный Участником в распоряжении Участника на возврат остатка гарантийного взноса, не позднее 2 (двух) рабочих дней после получения Оператором соответствующего распоряжения Участника.

4.11.3 Участник в течение 2 (двух) рабочих дней с даты прекращения участия удаляет надписи, вывески и иные предоставленные Оператором материалы, содержащие наименование Платежной Системы, и прекращает информировать клиентов об оказании Участником Услуг.

4.11.4 Участник обязан в течение шести месяцев с даты прекращения участия переадресовывать все телефонные звонки и обращения клиентов по поводу Услуг в СПК.

4.11.5 Участник обязан в течение 2 (двух) рабочих дней с даты прекращения участия удалить программное обеспечение Платежной Системы и возможность доступа к нему со всех компьютеров и серверов Участника (его Агента).

4.12 Права на средства индивидуализации

4.12.1 Все фирменные наименования, товарные знаки, знаки обслуживания, авторские права и прочие имущественные права Оператора, Операторов УПИ и/или любого аффилированного лица Оператора или Оператора УПИ в любой момент времени остаются их интеллектуальной собственностью , и Участник не имеет права в период участия в Платежной Системе или по его истечении заявлять на них какие-либо требования или предпринимать попытки зарегистрировать на свое имя какие-либо товарные знаки, обозначения, технологии или любые иные объекты интеллектуальной собственности Оператора, Оператора УПИ и/или любого аффилированного лица Оператора, Оператора УПИ или технологического подрядчика Оператора или Оператора УПИ.

4.12.2 Для целей оказания Услуг Участнику предоставляются права использовать наименование Платежной Системы и логотипы Платежной Системы, предоставленные Оператором Участникам. Указанные права не могут быть переданы Участником какому-либо третьему лицу. Права на использование наименования Платежной Системы и логотипов Платежной Системы предоставляются Участнику в течение всего периода участия Участника в Платежной Системе и автоматически прекращаются в момент прекращения участия Участника в Платежной Системе. Согласие на предоставление указанного права может быть отозвано Оператором в любое время путем направления Участнику соответствующего письменного уведомления. Настоящие Правила не предоставляют Участнику каких-либо прав на использование наименования Платежной Системы полностью или частично в доменных именах, а также на размещение унифицированных указателей ресурса (URL ссылок) или тегов на такие доменные имена.

Глава 5. Операторы Услуг Платежной Инфраструктуры

5.1 Порядок привлечения Операторов Услуг Платежной Инфраструктуры

5.1.1 В рамках Платежной Системы Операторами Услуг Платежной Инфраструктуры являются Операционный Центр, Центральный Платежный Клиринговый Контрагент и Расчетный Центр.

Операторы Услуг Платежной Инфраструктуры привлекаются Оператором на основании договоров между Оператором и соответствующими Операторами Услуг Платежной Инфраструктуры. Заключение договоров об оказании Услуг Платежного Клиринга и/или Операционных Услуг между Участниками и Оператором Услуг Платежной Инфраструктуры не является обязательным.

5.1.2 Функции ОЦ, ЦПКК и РЦ могут совмещаться одним Оператором Услуг Платежной Инфраструктуры, при условии соответствия такого Оператора Услуг Платежной Инфраструктуры требованиям законодательства и настоящим Правилам.

5.1.3 Оператор ведет перечень Операторов Услуг Платежной Инфраструктуры. В случае каких-либо изменений в перечне Операторов Услуг Платежной Инфраструктуры Оператор вносит соответствующие изменения в перечень Операторов Услуг Платежной Инфраструктуры не позднее, чем в день вступления в силу таких изменений. Перечень Операторов Услуг Платежной Инфраструктуры включает наименование, направление деятельности, место нахождения (адрес) и адрес официального сайта в сети Интернет по каждому из Операторов Платежной Инфраструктуры. Оператор получает информацию для включения в перечень Операторов Услуг Платежной Инфраструктуры непосредственно от Операторов Услуг Платежной Инфраструктуры при привлечении соответствующего Оператора Услуг Платежной Инфраструктуры. Для дальнейшей актуализации информации в перечне, Оператор включает в договоры с Операторами Услуг Платежной Инфраструктуры положения, обязывающие Оператора Услуг Платежной Инфраструктуры своевременно направлять Оператору обновленную информацию об Операторе Услуг Платежной Инфраструктуре в случае ее изменения. В случае прекращения работы какого-либо Оператора Услуг Платежной Инфраструктуры в Платежной Системе, Оператор исключает информацию о таком Операторе Услуг Платежной Инфраструктуры из перечня не позднее дня прекращения работы такого Оператора Услуг Платежной Инфраструктуры в Платежной Системе.

5.1.4 Требования к Операторам Услуг Платежной Инфраструктуры.

5.1.4.1 Оператор УПИ:

i) осуществляет свою деятельность в соответствии с законодательством Российской Федерации;

ii) имеет возможность оказывать Операционные Услуги и (или) Расчетные Услуги и (или) Услуги Платежного Клиринга в соответствии с законодательством Российской Федерации и настоящими Правилами. Для целей оказания Расчетных Услуг Оператор привлекает РЦ, являющийся кредитной организацией, которая не менее 1 (Одного) года осуществляет перевод денежных средств по открытым в этой кредитной организации банковским счетам;

iii) обладает финансовой устойчивостью (отсутствуют случаи нарушения обязательных нормативов в течение предшествующих 12 месяцев);

iv) обеспечивает защиту информации при осуществлении переводов денежных средств в соответствии с требованиями, установленными законодательством и нормативными актами Банка России для Операторов Услуг Платежной Инфраструктуры, а также в соответствии с настоящими Правилами;

v) техническая инфраструктура Оператора УПИ соответствует обязательным требованиям законодательства и требованиями нормативных актов Банка России, установленным для операторов услуг платежной инфраструктуры;

vi) Оператор УПИ подтверждает готовность выполнять требования Главы 8 Правил в части требований к Операторам УПИ.

5.2 Оплата услуг Операторов Услуг Платежной Инфраструктуры

5.2.1 Стоимость услуг Операторов Услуг Платежной Инфраструктуры оплачивается Оператором.

5.3 Права и обязанности ОЦ и ЦПКК

5.3.1 ОЦ обязан:

i) предоставлять Участнику доступ в Платежную Систему способами, определенными в Оферте;

ii) в случае если способ предоставления Участнику доступа в Платежную Систему требует предоставления Участнику дополнительного программного обеспечения Оператора, предоставлять Участнику такое программное обеспечение, в том числе идентификационные сертификаты, наименования пользователей (логин) и первичные пароли для доступа в Платежную Систему;

iii) осуществлять регистрацию Отделений;

iv) информировать Участника о фактах возникновения/устранения технических проблем и сбоев в работе Платежной Системы в случаях и порядке, определенных в настоящих Правилах;

v) обеспечивать подтверждение приема распоряжения Участника путем обеспечения присвоения КНДП переводу денежных средств клиента Участника;

vi) обеспечивать возможность осуществления исполнения перевода денежных средств клиента с момента присвоения такому переводу КНДП;

vii) обрабатывать информацию, поступившую в Платежную Систему от Участника в режиме реального времени;

viii) консультировать Участника по телефону по техническим вопросам, возникающим у Участника при работе в Платежной Системе;

5.3.2 ЦПКК обязан:

i. по рабочим дням предоставлять Участнику отчет о переводах, отправленных и выплаченных Участником, в соответствии с порядком платежного клиринга и расчета в Платежной Системе;

ii. определять платежные клиринговые позиции Участника в соответствии с порядком платежного клиринга и расчета в Платежной Системе;

iii. передавать в РЦ для исполнения распоряжения на сумму определенных платежных клиринговых позиций в соответствии с порядком платежного клиринга и расчета в Платежной Системе;

iv. вести учет гарантийных взносов Участников;

v. обладать денежными средствами, достаточными для исполнения своих обязательств, либо обеспечивать исполнение своих обязательств, в том числе за счет Гарантийного фонда Платежной Системы, в размере наибольшего обязательства, по которому ЦПКК становится плательщиком, за период, определяемый в соответствии с порядком платежного клиринга и расчета в Платежной Системе;

vi. ежедневно осуществлять контроль за рисками неисполнения (ненадлежащего исполнения) Участниками своих обязательств по переводу денежных средств, применять в отношении Участников, анализ финансового состояния которых свидетельствует о повышенном риске, ограничительные меры, включая установление максимального размера платежной клиринговой позиции, и предъявлять требования о повышенном размере обеспечения исполнения обязательств Участников;

vii. нести иные обязательства, прямо предусмотренные законодательством Российской Федерации и настоящими Правилами.

viii. При этом для выполнения обязанностей, ЦПКК на ежедневной основе осуществляет управление ликвидностью, что позволяет поддерживать достаточный объем денежных средств для исполнения обязательств ЦПКК, и управление кредитным риском, позволяющее контролировать риск неисполнения (ненадлежащего исполнения) обязательств Участниками. Управление ликвидностью и кредитным риском осуществляется в следующем порядке:

постоянный мониторинг и планирование потребности в ликвидных денежных средствах. В случае возникновения «конфликта интересов» между ликвидностью и прибыльностью всегда принимается решение в пользу ликвидности;

установление контрольных значений ликвидности;

контроль достаточности денежных средств на корреспондентских счетах ЦПКК;

установление предельных лимитов обязательств Участника с учетом уровня кредитного риска каждого Участника Платежной Системы;

создание Гарантийного фонда Платежной Системы за счет денежных средств Участников и его использование в случае неисполнения (ненадлежащего исполнения) Участниками своих обязательств.

5.3.3 ОЦ имеет право:

i) модернизировать, обновлять и изменять программное обеспечение, используемое Оператором;

ii) определять способы предоставления Участнику доступа в Платежную Систему;

iii) пользоваться иными правами, предусмотренными законодательством Российской Федерации и настоящими Правилами.

5.3.4 ЦПКК имеет право:

i. распоряжаться средствами гарантийного фонда Платежной Системы в соответствии с порядком платежного клиринга и расчета в Платежной Системе, а также с иными положениями настоящих Правил;

ii. пользоваться иными правами, предусмотренными законодательством Российской Федерации и настоящими Правилами.

5.4 Права и обязанности Расчетного Центра

5.4.1 РЦ обязан:

i) осуществлять деятельность РЦ в соответствии с законодательством Российской Федерации, настоящими Правилами, а также договорами банковского счета между РЦ и Участниками;

ii) в соответствии с требованиями законодательства Российской Федерации и внутренними процедурами, установленными РЦ, при открытии банковских счетов Участникам проводить в отношении Участников соответствующие проверочные мероприятия с целью ПОД/ФТ/ФРОМУ. По результатам проверочных мероприятий принимать решение о возможности открытия банковского счета Участнику;

iii) при заключении договоров банковского счета с Участниками включать в них:

а) положение о праве на списание денежных средств с банковского счета Участника без распоряжения Участника на условиях заранее данного акцепта при предъявлении распоряжения о списании со стороны ЦПКК в соответствии с порядком платежного клиринга и расчета в Платежной Системе;

б) требование исполнения обязанности Участника поддерживать на своем банковском счете остаток денежных средств в размере, необходимом для бесперебойного осуществления расчетов с ЦПКК;

iv) обеспечить исполнение распоряжений на проведение операций списания или зачисления денежных средств по банковским счетам Участников в соответствии с порядком платежного клиринга и расчета в Платежной Системе;

v) направлять Участникам подтверждения, касающиеся исполнения распоряжений Участников;

vi) нести иные обязательства, прямо предусмотренные законодательством Российской Федерации и настоящими Правилами.

5.4.2 РЦ имеет право:

i) самостоятельно определять и контролировать условия, порядок открытия и ведения

банковских счетов Участников, за исключением условий, установленных в настоящих Правилах;

ii) пользоваться иными правами, предусмотренными законодательством Российской Федерации и настоящими Правилами.

5.4.3 Требования к технологическому обеспечению РЦ

5.4.3.1 РЦ обязан использовать оборудование и программное обеспечение, соответствующее требованиям, установленным законодательством Российской Федерации в отношении оборудования и программного обеспечения, используемого для осуществления банковских операций.

5.4.3.2 РЦ обеспечивает наличие следующего оборудования и программного обеспечения:

а) Оборудование и программное обеспечение, позволяющие получать, обрабатывать и отправлять документы в формате TXT или XML;

б) Оборудование и программное обеспечение, позволяющие обеспечивать адекватную защиту информации, получаемой РЦ при выполнении им своим функций.

5.5 Порядок взаимодействия между Оператором, Участниками и Операторами Услуг Платежной Инфраструктуры

5.5.1 Взаимодействие между Оператором, Участниками и Операторами Услуг Платежной Инфраструктуры осуществляется в соответствии с правами и обязанностями Оператора, Участника и РЦ и ЦПКК, предусмотренными законодательством Российской Федерации, настоящими Правилами и/или договорами, предусмотренными настоящими Правилами.

5.6 Порядок предоставления Участниками Оператору информации о своей деятельности

5.6.1 Участники (в т.ч. в ходе ежедневного взаимодействия с Оператором) предоставляют информацию Оператору о своей деятельности:

а) в порядке и случаях, предусмотренных следующими положениями настоящих Правил:

- при направлении Участником Оператору заявления на участие в Платежной Системе (пункты 4.2.2, 4.2.3 настоящих Правил);
- в случае возникновения обстоятельств, временно препятствующих продолжению оказания Услуг, в день возникновения таких обстоятельств (пункт 4.4. настоящих Правил);
- при информировании Оператора об изменении фактического местонахождения, наименования Участника, а также о смене единоличного исполнительного органа Участника, в течение двух недель после вступления в силу таких изменений, а также своевременное информирование при смене почтового адреса, номера факсимильной связи, адресов электронной почты для направления уведомлений и иной информации, связанной с работой Участника в Платежной Системе (пункт 4.4. настоящих Правил);
- по запросу Оператора любой документации, касающейся переводов денежных средств, осуществленных Участником в рамках Платежной Системы, немедленно по первому требованию (пункт 4.4. настоящих Правил);
- по запросу Оператора информации по применяемым Участником (Агентами) процедурам в области ПОД/ФТ/ФРОМУ в случаях, когда предоставление такой информации не противоречит действующему законодательству Российской Федерации (пункт 4.4. настоящих Правил);
- по запросу Оператора финансовой отчетности Участника по формам 0409101, 0409123 и 0409135, а также финансовой отчетности Участника по форме 0409102, в течение 3 (трех) рабочих дней после получения Участником соответствующего запроса Оператора (пункт 4.4. настоящих Правил);
- в случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе не несущего финансовых последствий, но затрагивающего технологические участки, в срок не позднее 24

часов с момента возникновения (выявления) инцидента, а также в течение 24 часов после его устранения (пункт 8.14.1 настоящих Правил);

- в случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе несущего финансовые последствия, незамедлительно, но не позднее одного часа с момента выявления инцидента (пункт 8.14.1 настоящих Правил);
- регулярно для целей анализа обеспечения в Платежной Системе защиты информации при осуществлении переводов денежных средств и расчета показателей уровня риска информационной безопасности, на ежеквартальной основе не позднее пятнадцатого рабочего дня месяца, следующего за отчетным кварталом (пункт 8.14.2 настоящих Правил);
- по итогам проведения оценки соответствия уровням защиты информации (пункт 8.17 настоящих Правил);
- По запросу Оператора в целях управления рисками в Платежной Системе (пункт 9.8.1. настоящих Правил);
- по запросу Оператора о предоставлении информации, касающейся деятельности Участника в качестве субъекта Платежной Системы для целей оценки рисков и влияния на БФПС в Платежной Системе (Порядок обеспечения БФПС);
- при сборе Оператором данных и информации об Участниках в рамках программы «Знай своего клиента» (пункт 10.1.4 настоящих Правил);
- при осуществлении Оператором контроля за соблюдением Правил Участниками (пункты 11.2.1 – 11.2.3 настоящих Правил);
- при воздействии обстоятельств непреодолимой силы, в течение одного рабочего дня с момента возникновения указанных обстоятельств в устной форме и в течение трех рабочих дней в письменной форме (пункт 11.6 настоящих Правил);
- в случае выявления Участником в рамках Платежной Системы чрезвычайных ситуаций, в том числе, событий, вызвавших системные сбои, незамедлительно (пункт 13.1 настоящих Правил);
- в порядке и случаях, предусмотренных законодательством Российской Федерации, а также в иных случаях, предусмотренных настоящими Правилами).

5.6.2 Участники предоставляют информацию о своей деятельности с использованием следующих каналов/способов передачи информации:

а) электронная почта;
б) бумажные носители;
в) телефонная связь;
г) в устной форме во время личных встреч;
д) через иные заранее согласованные Участником и Оператором каналы связи.

5.6.3. Адреса электронной почты и номера телефонов для использования Участниками в целях, указанных в п. 5.6.1. предоставляются Оператором Участнику до начала Участником работы в рамках Платежной Системы. В случае изменения указанных номеров телефонов и адресов электронной почты, Оператор уведомит Участников о таких изменениях путем направления уведомления в письменном виде или путем направления информации на адрес электронной почты Участника или путем размещения соответствующей информации на сайте Оператора www.omnypay.ru.

5.7 Конфиденциальность

5.7.1 Оператор, Операторы Услуг Платежной Инфраструктуры и Участники гарантируют сохранение конфиденциальности получаемых и передаваемых в рамках Платежной Системы данных, информации, документов (в том числе условия Оферты), программного обеспечения, кодов и паролей, персональных данных отправителей и получателей переводов денежных средств, данных об объеме операций Участника в рамках Платежной Системы , а также иной информации, составляющей банковскую, коммерческую или иную охраняемую законом тайну (далее «**Конфиденциальная информация**»). При привлечении Агентов Участник обязуется обеспечить соблюдение такими

Агентами режима конфиденциальности в отношении Конфиденциальной информации, к которой такие Агенты будут иметь доступ.

5.7.2 Оператор, Операторы Услуг Платежной Инфраструктуры и Участники имеют право раскрывать Конфиденциальную информацию:

а) в целях исполнения своих обязанностей в рамках Платежной Системы;

б) в целях осуществления перевода денежных средств;

в) в случаях и порядке, предусмотренных настоящими Правилами;

г) в случаях и порядке, предусмотренных законодательством Российской Федерации;

д) с письменного согласия лица, предоставившего Конфиденциальную информацию раскрывающему лицу, в случае если такое раскрытие не противоречит законодательству Российской Федерации и не нарушает права и законные интересы третьих лиц.

5.7.3 Оператор, Операторы Услуг Платежной Инфраструктуры и Участники гарантируют банковскую тайну в соответствии с законодательством Российской Федерации.

5.7.4 Режим конфиденциальности Конфиденциальной информации обеспечивается субъектами Платежной Системы в течение всего срока сохранения ими статуса субъектов Платежной Системы и в течение 10 (десяти) лет после утраты статуса субъекта Платежной Системы.

5.8 Временной регламент функционирования Платежной Системы

5.8.1 Рабочими днями Оператора являются рабочие дни, установленные законодательством Российской Федерации. Рабочим временем Оператора является промежуток времени с 9.00 часов по 18.00 часов московского времени. Участники могут связаться с СПК для получения консультации семь дней в неделю по телефону, размещенному на сайте www.omnypay.ru в течение часов работы СПК.

5.8.2 Внутренним временем работы процессинга Платежной Системы является московское время.

5.8.3 Прием к исполнению распоряжений Участников осуществляется круглосуточно, в том числе в выходные и праздничные дни.

5.8.4 Для целей осуществления клиринга и расчетов используется московское время.

5.8.5 Расчеты в рамках Платежной Системы осуществляются исключительно по рабочим дням.

Глава 6. Порядок осуществления платежного клиринга и расчета в рамках Платежной Системы

6.1 Общие положения

6.1.1 Платежный клиринг в Платежной Системе осуществляется ЦПКК посредством:

а) выполнения процедур приема к исполнению распоряжений Участников, включая проверку соответствия распоряжений Участников установленным требованиям, определение достаточности денежных средств для исполнения распоряжений Участников и определение платежных клиринговых позиций;

б) передачи РЦ для исполнения принятых распоряжений Участников;

в) направления Участникам извещений (подтверждений), касающихся приема к исполнению распоряжений Участников, а также передачи извещений (подтверждений), касающихся исполнения распоряжений Участников.

6.1.2 Распоряжение Участника, по которому Участник является плательщиком денежных средств (при отправлении перевода денежных средств клиентом Участника), считается принятым ЦПКК с момента присвоения переводу денежных средств КНДП. Присвоение КНДП является подтверждением соответствия распоряжения Участника установленным требованиям и факта принятия и исполнения ЦПКК такого распоряжения Участника.

6.1.3 Распоряжение Участника, по которому Участник является получателем денежных средств (при выплате перевода денежных средств клиенту Участника), считается принятым ЦПКК с момента изменения статуса перевода денежных средств в процессинге Платежной Системы на «paid»

(«Выплачен»). Изменение статуса перевода денежных средств на «paid» («Выплачен») является подтверждением соответствия распоряжения Участника установленным требованиям и факта принятия и исполнения ЦПКК такого распоряжения Участника.

6.1.4 В целях управления кредитным риском, а также в целях обеспечения достаточности денежных средств для исполнения распоряжений распоряжения Участника, по которым Участник является плательщиком денежных средств (при отправлении перевода денежных средств клиентом Участника), принимаются к исполнению с учетом лимитов, установленных ЦПКК в соответствии с настоящими Правилами и условиями Оферты.

6.1.5 Определение платежной клиринговой позиции Участника осуществляется ЦПКК на нетто-основе по каждой из валют расчета.

6.1.6 Платежная клиринговая позиция Участника определяется ЦПКК в сроки и в порядке, определенные в настоящей Главе, с учетом следующих особенностей:

а) с момента принятия ЦПКК распоряжения Участника, по которому Участник является плательщиком денежных средств (при отправлении перевода денежных средств клиентом Участника), ЦПКК увеличивает расчетные обязательства Участника перед ЦПКК на сумму перевода денежных средств и Платы за перевод (в случае ее взимания Участником) за вычетом вознаграждения Участника, причитающегося Участнику за отправление перевода денежных средств в соответствии с Офертой;

б) с момента принятия ЦПКК распоряжения Участника, по которому Участник является получателем денежных средств (при выплате перевода денежных средств клиенту Участника), ЦПКК увеличивает расчетные обязательства ЦПКК перед Участником на сумму перевода денежных средств и вознаграждение Участника, причитающегося Участнику за выплату перевода денежных средств в соответствии с Офертой;

в) платежная клиринговая позиция Участника, на основании которой ЦПКК направляет распоряжение в РЦ для исполнения, определяется ЦПКК как разница между расчетными обязательствами Участника перед ЦПКК и расчетными обязательствами ЦПКК перед Участником за определенный в соответствии с настоящей Главой 6 период времени.

6.1.7 В качестве единой шкалы времени для целей осуществления платежного клиринга и расчета признается московское время. Контрольным является время системных часов аппаратных средств ЦПКК.

6.1.8 Платежный клиринг и расчет осуществляются по рабочим дням, установленным в соответствии с законодательством Российской Федерации, с 9.00 часов до 18.00 часов по московскому времени – с понедельника по четверг и с 9.00 часов до 17.00 часов – в пятницу и предпраздничные дни.

6.1.9 Расчеты в Платежной Системе осуществляются в российских рублях и долларах США.

6.1.10 Для целей платежного клиринга и расчета платежная клиринговая позиция определяется ЦПКК по каждой из валют расчета. Определение платежной клиринговой позиции по распоряжениям Участника, полученным ЦПКК в разных валютах, в одной валюте расчета, а также дальнейший расчет по таким распоряжениям в одной валюте расчета возможны только в случаях, прямо предусмотренных настоящими Правилами или законодательством Российской Федерации.

6.1.11 ЦПКК по рабочим дням, после завершения каждого календарного дня, предоставляет Участнику в электронной форме отчетную информацию по всем распоряжениям Участника, принятым ЦПКК (далее «**Отчет о переводах**»). Отчет о переводах составляется на основе данных, поступивших в Платежную Систему от Участника. Описание формата Отчета о переводах указывается ЦПКК в составе Инструктивных материалов, предоставляемых ЦПКК Участнику. ЦПКК заблаговременно уведомляет Участника об изменении формата Отчета о переводах. Отчет о переводах содержит информацию, являющуюся основанием для расчета.

6.2 Сроки и порядок осуществления платежного клиринга и расчета Участниками.

6.2.1 Платежная клиринговая позиция Участника для целей расчетов определяется ЦПКК путем учета всех распоряжений Участника, поступивших за отчетный период в каждой из валют расчета (далее «**Отчетный период**»). Отчетный период определяется как промежуток (промежутки) времени с 00.00 часов до 24.00 часов по московскому времени в течение одного рабочего дня и всех нерабочих

дней, непосредственно следующих за таким рабочим днем. В случае если сумма платежной клиринговой позиции Участника (нетто расчетные обязательства Участника перед ЦПКК или нетто расчетные обязательства ЦПКК перед Участником), определенная ЦПКК за Отчетный период в одной из валют расчета, превышает пороговую величину задолженности, указанную ЦПКК в Оферте (далее «**Пороговая величина**»), ЦПКК направляет в РЦ распоряжение на сумму платежной клиринговой позиции. Если сумма платежной клиринговой позиции Участника (нетто расчетные обязательства Участника перед ЦПКК или нетто расчетные обязательства ЦПКК перед Участником), определенная ЦПКК за Отчетный период в одной из валют расчета, не превышает Пороговую величину, Отчетный период продлевается включительно по день, по состоянию на конец которого сумма платежной клиринговой позиции Участника (нетто расчетные обязательства Участника перед ЦПКК или нетто расчетные обязательства ЦПКК перед Участником) достигнет или превысит Пороговую величину. При этом, если окончание такого продленного периода приходится на нерабочий день, в отчетный период включаются все нерабочие дни, непосредственно следующие за таким нерабочим днем. В случае, если сумма платежной клиринговой позиции Участника (нетто расчетные обязательства Участника перед ЦПКК или нетто расчетные обязательства ЦПКК перед Участником), определенная ЦПКК в одной из валют расчета за Отчетный период свыше 10 (десяти) дней, не превышает Пороговую величину, ЦПКК вправе направить в РЦ распоряжение на сумму такой платежной клиринговой позиции При этом, последним днем соответствующего Отчетного периода является день, предшествующий дню определения ЦПКК платежной клиринговой позиции Участника.

В целях минимизации рисков Платежной Системы ЦПКК вправе определить промежуточную платежную клиринговую позицию Участника до окончания текущего операционного дня и направить в этот же день в РЦ распоряжение на сумму такой платежной клиринговой позиции. При этом сумма распоряжения, направляемого в РЦ, может быть скорректирована ЦПКК в зависимости от наличия / отсутствия достаточного остатка денежных средств на банковском счете Участника в РЦ. Определение итоговой платежной клиринговой позиции Участника и проведение окончательного взаиморасчета осуществляется ЦПКК не позднее дня, следующего за днем определения промежуточной платежной клиринговой позиции.

В случае определения ЦПКК промежуточной платежной клиринговой позиции Участника, РЦ вправе либо осуществить полный расчет по такой платежной клиринговой позиции при условии наличия достаточного остатка денежных средств на банковском счете Участника в РЦ, либо осуществить частичный расчет в пределах остатка денежных средств на банковском счете Участника. В случае осуществления частичного расчета по промежуточной платежной клиринговой позиции, сумма непогашенных обязательств не признается просроченной задолженностью при условии ее погашения в момент осуществления расчета по итоговой платежной клиринговой позиции. Исполнение итоговой платежной клиринговой позиции или признание ее просроченной задолженностью осуществляется в соответствии с п. 6.2.4 настоящих Правил.

6.2.2 Положительная платежная клиринговая позиция Участника означает расчетные обязательства ЦПКК перед Участником, подлежащие исполнению путем зачисления денежных средств на корреспондентский счет Участника, открытый в РЦ.

6.2.3 Отрицательная платежная клиринговая позиция Участника означает расчетные обязательства Участника перед ЦПКК, подлежащие исполнению путем списания денежных средств с корреспондентского счета Участника, открытого в РЦ.

6.2.4 Участники обязаны обеспечить не позднее 16 часов по московскому времени достаточный остаток денежных средств на своих корреспондентских счетах, открытых в РЦ, для исполнения положительных клиринговых позиций в каждой валюте расчета. РЦ обязан обеспечить наличие на своих корреспондентских счетах денежных средств в сумме, необходимой для исполнения всех положительных платежных клиринговых позиций Участников. В случае неисполнения (или несвоевременного исполнения) своих обязательств по обеспечению достаточного остатка денежных средств, а также, если такое неисполнение повлекло за собой невозможность полного исполнения платежной клиринговой позиции, такая неисполненная платежная клиринговая позиция признается просроченной задолженностью.

6.2.5 Платежные клиринговые позиции исполняются РЦ путем списания и зачисления

денежных средств на корреспондентские счета Участников, открытые в РЦ, в период с 15.00 часов по 18.00 часов московского времени в рабочие дни РЦ.

6.2.6 В случае, если Участник не обеспечил остаток денежных средств на корреспондентском счете (счетах), необходимых для исполнения отрицательных платежных клиринговых позиций (за исключением случаев исполнения промежуточных платежных клиринговых позиций), РЦ вправе:

а) исполнить отрицательную платежную клиринговую позицию (полностью или частично) за счет средств гарантийного взноса Участника с последующим уменьшением постоянного дневного лимита Участника и направлением требования Участнику о пополнении гарантийного взноса. При этом, ЦПКК вправе осуществить перерасчет отрицательной платежной клиринговой позиции из одной валюты в другую (полностью или частично) по курсу Банка России, установленному на день перерасчета; и (или)

а) осуществить перерасчет отрицательной платежной клиринговой позиции из одной валюты в другую (полностью или частично) по курсу Банка России, установленному на день перерасчета, и сформировать новую отрицательную платежную клиринговую позицию для исполнения в пределах данного рабочего дня; и (или)

б) направить Участнику требование о пополнении корреспондентского счета (счетов) Участника, открытого (открытых) в РЦ; и (или)

в) исполнить отрицательную платежную клиринговую позицию частично в пределах остатка денежных средств, имеющихся на корреспондентском счете Участника в РЦ.

При этом, ЦПКК имеет право исполнить отрицательную платежную клиринговую позицию (полностью или частично) за счет средств гарантийного взноса Участника с последующим уменьшением постоянного дневного лимита Участника и направлением требования Участнику о пополнении гарантийного взноса. ЦПКК вправе осуществить перерасчет отрицательной платежной клиринговой позиции из одной валюты в другую (полностью или частично) по курсу Банка России, установленному на день перерасчета.

6.2.7 В случае выявления ЦПКК в процессе выполнения процедур по мониторингу кредитных рисков признаков ухудшения финансового состояния Участника, ЦПКК имеет право сформировать платежную клиринговую позицию до завершения Отчетного периода и провести расчеты с Участником в соответствии с настоящим п. 6.2 до завершения Отчетного периода.

Глава 7. Порядок обеспечения обязательств Участников по переводу денежных средств. Гарантийный фонд Платежной Системы

7.1 Порядок обеспечения обязательств Участников по переводу денежных средств

7.1.1 Обязательства Участников по переводу денежных средств в рамках Платежной Системы исполняются за счет:

а) средств Участников, находящихся на их счетах, открытых в РЦ;

б) средств гарантийного фонда Платежной Системы (далее «**Гарантийный фонд**»).

7.2 Гарантийный фонд

7.2.1 Гарантийный фонд создается ЦПКК за счет денежных средств Участников в целях обеспечения исполнения обязательств Участников.

7.2.2 Гарантийный фонд формируется путем перечисления Участниками ЦПКК гарантийных взносов, порядок определения которых определяется в соответствии с настоящими Правилами.

7.2.3 Гарантийные взносы Участников учитывается на отдельных банковских счетах, открытых Участниками в РЦ в валютах расчета в Платежной Системе.

7.2.4 Операции по указанному счету осуществляются на основании распоряжений ЦПКК.

7.2.5 Размер гарантийного взноса определяется в соответствии с порядком определения постоянного лимитов, устанавливаемых на Участника.

7.2.6 В случае неисполнения (ненадлежащего исполнения) обязательств Участником в рамках

Платежной Системы его гарантийный взнос используется для удовлетворения требований по таким обязательствам.

7.2.7 При недостаточности гарантийного взноса Участника для удовлетворения требований по обязательствам такого Участника в рамках Платежной Системы используются гарантийные взносы других Участников.

7.2.8 Решение об использовании гарантийных взносов Участников для целей удовлетворения требований по обязательствам Участника при недостаточности гарантийного взноса такого Участника для удовлетворения требований в полном объеме принимается ЦПКК самостоятельно. При этом, выбор используемых гарантийных взносов осуществляется ЦПКК с учетом платежных клиринговых позиций Участников, сформированных ЦПКК на день использования гарантийного взноса.

7.2.9 ЦПКК уведомит Участника об использовании его гарантийного взноса в целях, указанных в п. 7.2.7 настоящих Правил, не позднее следующего рабочего дня после использования гарантийного взноса Участника.

7.2.10 Участник, чьи обязательства были исполнены за счет гарантийных взносов других Участников, обязан возместить сумму использованных гарантийных взносов в течении 2 (двух) рабочих дней после удовлетворения требований по обязательствам такого Участника в рамках Платежной Системы.

7.2.11 В случае прекращения участия Участника в Платежной Системе, гарантийный взнос Участника возвращается Участнику в сроки и порядке, определенные в п. 4.11 настоящих Правил.

7.3 Порядок определения постоянного дневного лимита и расчета гарантийного взноса Участника

7.3.1 Постоянный дневной лимит на отправление денежных средств в Платежной Системе устанавливается на каждое Отделение, Интернет-банк, Терминал самообслуживания или на Участника в целом по решению ЦПКК.

7.3.2 В случае принятия ЦПКК решения об изменении способа установления постоянного дневного лимита ЦПКК уведомляет Участника о таком решении в письменной форме.

7.3.3 Сумма постоянного дневного лимита устанавливается в каждой из валют расчета.

7.3.4 Первоначальное значение постоянного дневного лимита устанавливается в Оферте. Дальнейшее изменение дневного лимита осуществляется по требованию ЦПКК в одностороннем порядке в соответствии с настоящими Правилами.

7.3.5 Без перечисления гарантийного взноса устанавливается значение дневного лимита в зависимости от количества Отделений. При этом Оператор указывает в Оферте максимальное значение общего дневного лимита на Участника без перечисления гарантийного взноса. Если постоянный дневной лимит устанавливается на каждое Отделение, то общая сумма постоянного дневного лимита, указанная в Оферте, распределяется между всеми Отделениями. Дневной лимит, устанавливаемый без перечисления Участником гарантийного взноса, может быть скорректирован в меньшую сторону в том случае, если по результатам проведенного анализа операций по отправлению перевода денежных средств за длительный период ЦПКК выявит, что Участник (или Отделение) в большинстве случаев не использует установленный постоянный дневной лимит.

7.3.6 Для установления (изменения) постоянного дневного лимита на отправление переводов денежных средств сумма гарантийного взноса по каждой из валют расчета определяется по следующей формуле:

$$A_n = L_n * a_n,$$

где:

A_n – сумма гарантийного взноса;

L_n – предельное значение лимита на отправление переводов денежных средств с учетом уровня риска на Участника.

a_n – коэффициент, определяемый в соответствии с Офертой в зависимости от уровня риска на

момент расчета гарантийного взноса ЦПКК.

7.3.7 Гарантийный взнос может быть перечислен Участником как в каждой валюте расчета отдельно, так и общей суммой в одной любой валюте расчета, причем пересчет одной валюты в другую осуществляется по курсу Банка России на день перечисления общей суммы гарантийного взноса на счет Участника. Общая сумма гарантийного взноса, перечисленная в одной из валют расчета, может быть пересмотрена и скорректирована по инициативе Участника или ЦПКК в случае, если текущий курс Банка России будет отличаться от курса на дату перечисления общей суммы гарантийного взноса более, чем на 15%.

Глава 8. Требования к защите информации при осуществлении переводов денежных средств в Платежной Системе

Оператор определяет в настоящих Правилах порядок обеспечения защиты информации в Платежной Системе для Участников и Операторов Услуг Платежной Инфраструктуры с учетом требований к обеспечению защиты информации при осуществлении переводов денежных средств.

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

управление риском информационной безопасности в Платежной Системе как одним из видов операционного риска в платежной системе, источниками реализации которого являются: недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации, недостатки прикладного программного обеспечения автоматизированных систем и приложений, а также несоблюдение требований к указанным процессам деятельности операторами по переводу денежных средств, являющимися Участниками, Операторами Услуг Платежной Инфраструктуры;

установление состава показателей уровня риска информационной безопасности в Платежной Системе;

реализация Операторами по переводу денежных средств, являющимися Участниками платежной системы, и Операторами Услуг Платежной Инфраструктуры механизмов, направленных на соблюдение требований к обеспечению защиты информации при осуществлении переводов денежных средств, и контроль их соблюдения операторами по переводу денежных средств, являющимися Участниками, и Операторами Услуг Платежной Инфраструктуры;

реализация операторами по переводу денежных средств, являющимися Участниками, и Операторами Услуг Платёжной Инфраструктуры процессов выявления и идентификации риска информационной безопасности в платежной системе в отношении объектов информационной инфраструктуры Участников, Операторов Услуг Платежной Инфраструктуры;

выявление и анализ операторами по переводу денежных средств, являющимися Участниками, и Операторами Услуг Платежной Инфраструктуры риска информационной безопасности в платежной системе;

реализация операторами по переводу денежных средств, являющимися Участниками Платежной Системы, и Операторами Услуг Платежной Инфраструктуры процессов реагирования на инциденты защиты информации и восстановления штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации;

реализация операторами по переводу денежных средств, являющимися Участниками, и Операторами Услуг Платежной Инфраструктуры взаимодействия при обмене информацией об инцидентах защиты информации;

реализация операторами по переводу денежных средств, являющимися Участниками, и Операторами Услуг Платежной Инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента, определенных пунктами 3.2 и 3.4 Указания Банка России от 9 января 2023 года № 6354-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами платежных платформ в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, форме и порядке получения ими от

Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента», зарегистрированного Министерством юстиции Российской Федерации 25 мая 2023 года № 73472;

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

8.1 Информация, подлежащая защите при осуществлении переводов денежных средств

Требования к обеспечению защиты информации при осуществлении переводов денежных средств применяются для обеспечения защиты следующей информации (далее - защищаемая информация):

1) информации об остатках денежных средств на банковских счетах;

2) 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;

3) информации, содержащейся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов Участников (далее - клиентов), распоряжениях Участников, распоряжениях платежного клирингового центра;

4) информации, содержащейся в электронных сообщениях, передаваемых при взаимодействии Участников, Агентов и Оператора, в том числе в электронных сообщениях, составленных Агентами от имени Участника;

5) информации о платежных клиринговых позициях;

6) информации, содержащейся в реестрах, сформированных на основе электронных сообщений;

7) информации, необходимой для удостоверения клиентами права распоряжения денежными средствами, в том числе данных держателей платежных карт;

8) информации, используемой для идентификации, аутентификации и авторизации работников Участников при осуществлении переводов денежных средств;

9) ключевой информации средств криптографической защиты информации (далее - СКЗИ), используемых при осуществлении переводов денежных средств (далее - криптографические ключи);

10) информации о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Участником, Оператором Услуг Платежной Инфраструктуры, Агентом и используемых для осуществления переводов денежных средств (далее - объекты информационной инфраструктуры), а также информации о конфигурации, определяющей параметры работы технических средств по защите информации;

11) информации ограниченного доступа, в том числе персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, обрабатываемой при осуществлении переводов денежных средств.

8.2 Требования к обеспечению защиты информации при осуществлении переводов денежных средств

Требования к обеспечению защиты информации при осуществлении переводов денежных средств включают в себя:

1) требования к организации и функционированию подразделения (работников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации (далее - служба информационной безопасности);

2) требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации на стадиях жизненного цикла объектов информационной инфраструктуры;

3) требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при назначении и распределении функциональных прав и обязанностей (далее - ролей) лиц, связанных с осуществлением переводов денежных средств;

4) требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при осуществлении доступа к объектам информационной инфраструктуры, включая требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от несанкционированного доступа;

5) требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации от воздействия программных кодов, приводящих к нарушению штатного функционирования средства вычислительной техники (далее - вредоносный код);

6) требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании информационно-телекоммуникационной сети Интернет (далее - сеть Интернет) при осуществлении переводов денежных средств;

7) требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании СКЗИ;

8) требования к обеспечению защиты информации при осуществлении переводов денежных средств с использованием взаимоувязанной совокупности организационных мер защиты информации и технических средств защиты информации, применяемых для контроля выполнения технологии обработки защищаемой информации при осуществлении переводов денежных средств (далее - технологические меры защиты информации);

9) требования к обеспечению защиты среды виртуализации при осуществлении переводов денежных средств Участником, Агентом, являющимся юридическим лицом, Оператором Услуг Платежной Инфраструктуры;

10) требования к повышению осведомленности работников Участника, Агента, являющегося юридическим лицом, Оператора Услуг Платежной Инфраструктуры и клиентов (далее - повышение осведомленности) в области обеспечения защиты информации;

11) требования к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагированию на них и восстановлению штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации, а также мероприятий по реализации взаимодействия при обмене информацией об инцидентах защиты информации;

12) требования к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;

13) требования к совершенствованию Оператором, Участником, Оператором Услуг Платежной Инфраструктуры защиты информации при осуществлении переводов денежных средств;

14) требования к оценке выполнения Оператором, Участником, Оператором Услуг Платежной Инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств;

15) требования к доведению Участником, Оператором Услуг Платежной Инфраструктуры до Оператора информации об обеспечении в Платежной Системе защиты информации при осуществлении переводов денежных средств;

16) требования по противодействию осуществлению переводов денежных средств без согласия клиента;

17) требования к управлению риском информационной безопасности, а также выявления и идентификации риска информационной безопасности Участником, Оператором Услуг Платежной Инфраструктуры

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

Выполнение требований к обеспечению защиты информации при осуществлении переводов денежных средств обеспечивается путем:

1) выбора организационных мер защиты информации; определения во внутренних документах Участника, Агента, Оператора, Оператора Услуг Платежной Инфраструктуры порядка применения организационных мер защиты информации; определения лиц, ответственных за применение организационных мер защиты информации; применения организационных мер защиты; реализации контроля применения организационных мер защиты информации; выполнения иных необходимых действий, связанных с применением организационных мер защиты информации;

2) выбора технических средств защиты информации; определения во внутренних документах Участника, Агента, Оператора, Оператора Услуг Платежной Инфраструктуры порядка использования технических средств защиты информации, включающего информацию о конфигурации, определяющую параметры работы технических средств защиты информации; назначения лиц, ответственных за использование технических средств защиты информации; использования технических средств защиты информации; реализации контроля за использованием технических средств защиты информации; выполнения иных необходимых действий, связанных с использованием технических средств защиты информации.

8.4 Состав требований к организации и функционированию службы информационной безопасности

В состав требований к организации и функционированию службы информационной безопасности включаются следующие требования:

1) Участник, Агент, являющийся юридическим лицом, Оператор Услуг Платежной Инфраструктуры:

i) обеспечивают формирование службы информационной безопасности, а также определяют во внутренних документах цели и задачи деятельности этой службы;

ii) предоставляют полномочия и выделяют ресурсы, необходимые для выполнения службой информационной безопасности установленных целей и задач.

2) Участник, имеющий филиалы:

i) обеспечивает формирование служб информационной безопасности в указанных филиалах, определяет для них необходимые полномочия и выделяет необходимые ресурсы;

ii) обеспечивает взаимодействие и координацию работ служб информационной безопасности.

3) Служба информационной безопасности осуществляет планирование и контроль обеспечения защиты информации при осуществлении переводов денежных средств, для чего наделяется следующими полномочиями:

i) осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств;

ii) определять требования к техническим средствам защиты информации и организационным мерам защиты информации;

iii) контролировать выполнение работниками требований к обеспечению защиты информации при осуществлении переводов денежных средств;

iv) участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации;

v) участвовать в действиях, связанных с выполнением требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых при восстановлении предоставления услуг платежной системы после сбоев и отказов в работе объектов информационной инфраструктуры.

8.5 Состав требований к обеспечению защиты информации при осуществлении переводов

денежных средств, применяемых для защиты информации на стадиях жизненного цикла объектов информационной инфраструктуры

В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации на стадиях жизненного цикла объектов информационной инфраструктуры, включаются следующие требования:

1) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств.

2) Участник, Агент, являющийся юридическим лицом, Оператор Услуг Платежной Инфраструктуры, обеспечивает участие службы информационной безопасности в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры.

3) Участник, Агент, являющийся юридическим лицом, Оператор Услуг Платежной Инфраструктуры, обеспечивают контроль со стороны службы информационной безопасности соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий.

4) Участник, Агент, Оператор Услуг Платежной Инфраструктуры, оператор услуг платежной инфраструктуры обеспечивают:

i) наличие эксплуатационной документации на используемые технические средства защиты информации;

ii) контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации;

iii) восстановление функционирования технических средств защиты информации, используемых при осуществлении переводов денежных средств, в случаях сбоев и (или) отказов в их работе.

5) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры.

6) Участник, Агент, Оператор Услуг Платежной Инфраструктуры на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают:

i) реализацию запрета несанкционированного копирования защищаемой информации;

ii) защиту резервных копий защищаемой информации;

iii) уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, Правилами и (или) договорами, заключенными Участником, Агентом, Оператором, Оператором Услуг Платежной Инфраструктуры;

iv) уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления.

8.6 Состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации при назначении и распределении ролей лиц, связанных с осуществлением переводов денежных средств

В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации при назначении и распределении ролей лиц, связанных с осуществлением переводов денежных средств, включаются следующие требования:

1) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают регистрацию лиц, обладающих правами: по осуществлению доступа к защищаемой информации; по управлению криптографическими ключами; по воздействию на объекты информационной инфраструктуры, которое может привести к нарушению предоставления услуг по осуществлению переводов денежных средств, за исключением банкоматов и платежных терминалов.

2) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают

регистрацию своих работников, обладающих правами по формированию электронных сообщений, содержащих распоряжения об осуществлении переводов денежных средств (далее - электронные сообщения).

3) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают реализацию запрета выполнения одним лицом в один момент времени следующих функций: эксплуатации и (или) контроля эксплуатации объекта информационно инфраструктуры, в том числе автоматизированных систем, одновременно с использованием по назначению объекта информационной инфраструктуры в рамках осуществления переводов денежных средств; создания и (или) модернизации объекта информационной инфраструктуры одновременно с использованием по назначению объекта информационной инфраструктуры в рамках осуществления переводов денежных средств; эксплуатации средств и систем защиты информации одновременно с контролем эксплуатации средств и систем защиты информации;

4) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают контроль и регистрацию действий лиц, которым назначены роли, определенные в настоящем пункте, в том числе эксплуатационного персонала;

8.7 Состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации при осуществлении доступа к объектам информационной инфраструктуры

В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации при осуществлении доступа к объектам информационной инфраструктуры, включаются следующие требования:

1) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают идентификацию, учет объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации, в том числе банкоматов и платежных терминалов.

2) При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных выше, Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают осуществление: логического доступа пользователям и эксплуатационным персоналом под уникальными и персонифицированными учетными записями; контроля соответствия фактического состава разблокированных учетных записей фактическому составу легальных субъектов логического доступа; контроля отсутствия незаблокированных учетных записей уволенных работников, работников, отсутствующих на рабочем месте более 90 календарных дней, работников внешних (подрядных) организаций, прекративших свою деятельность в организации; контроля отсутствия незаблокированных учетных записей неопределенного целевого назначения.

3) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают применение некриптографических средств защиты информации от несанкционированного доступа, в том числе имеющих подтверждение соответствия требованиям, установленным федеральным органом исполнительной власти в области обеспечения безопасности. Допускается применение некриптографических средств защиты информации от несанкционированного доступа иностранного производства.

4) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают: документарное определение правил предоставления (отзыва) и блокирования логического доступа; хранение эталонной информации о предоставленных правах логического доступа и обеспечение целостности этой информации; исключение возможного бесконтрольного самостоятельного расширения пользователями предоставленных им прав логического доступа; исключение бесконтрольного изменения пользователями параметров настроек средств и систем защиты информации, параметров настроек автоматизированных систем, связанных с защитой информации; назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации;

5) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают: контроль необходимости отзыва прав субъектов логического доступа при изменении их должностных

обязанностей; контроль прекращения предоставления логического доступа и блокирование учетных записей при истечении периода (срока) предоставления логического доступа;

6) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают: регистрацию выполнения субъектами логического доступа ряда неуспешных последовательных попыток аутентификации; регистрацию осуществления субъектами логического доступа идентификации и аутентификации4 регистрацию авторизации, завершения и (или) прерывания (приостановки) осуществления эксплуатационным персоналом и пользователями логического доступа; регистрацию изменений аутентификационных данных, используемых для осуществления логического доступа.

7) При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных выше, Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают: регистрацию действий клиентов, выполняемых с использованием программного обеспечения, входящего в состав объектов информационной инфраструктуры и используемого для осуществления переводов денежных средств (далее - программное обеспечение), и автоматизированных систем, входящих в состав объектов информационной инфраструктуры и используемых для осуществления переводов денежных средств (далее - автоматизированные системы), при наличии технической возможности; регистрацию действий, связанных с назначением и распределением прав клиентов, предоставленных им в автоматизированных системах и программном обеспечении, при наличии технической возможности.

8) При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных выше, Участник обеспечивает регистрацию действий с информацией о банковских счетах, включая операции открытия и закрытия банковских счетов.

9) Участник, Агент, Оператор Услуг Платежной Инфраструктуры принимают и фиксируют во внутренних документах решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, предназначенных для: контроля физического доступа к объектам информационной инфраструктуры (за исключением банкоматов и платежных терминалов), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, а также доступа в здания и помещения, в которых они размещаются; предотвращения физического воздействия на средства вычислительной техники, эксплуатация которых обеспечиваются Участником, Агентом, Оператором Услуг Платежной Инфраструктуры и которые используются для осуществления переводов денежных средств (далее - средства вычислительной техники), и телекоммуникационное оборудование, эксплуатация которого обеспечивается Участником, Агентом, Оператором Услуг Платежной Инфраструктуры и которое используется для осуществления переводов денежных средств (далее - телекоммуникационное оборудование), сбои и (или) отказы в работе которых приводят к невозможности предоставления услуг по переводу денежных средств или к несвоевременности осуществления переводов денежных средств, за исключением банкоматов и платежных терминалов;

10) В случае принятия Участником, Агентом, Оператором Услуг Платежной Инфраструктуры решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, указанных выше, Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают применение указанных организационных мер защиты информации и (или) использование указанных технических средств защиты информации.

11) Участник, Агент обеспечивают контроль отсутствия размещения на платежных терминалах и банкоматах специализированных средств, предназначенных для несанкционированного получения (съема) информации, необходимой для осуществления переводов денежных средств.

12) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают принятие мер, направленных на предотвращение хищений носителей защищаемой информации.

13) Участник обеспечивает возможность приостановления (блокирования) клиентом приема к исполнению распоряжений об осуществлении переводов денежных средств от имени указанного клиента.

8.8 Состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации от воздействия вредоносного кода

В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации от воздействия вредоносного кода, включаются следующие требования:

1) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают реализацию: защиты от вредоносного кода на уровне физических АРМ пользователей и эксплуатационного персонала; защиты от вредоносного кода на уровне виртуальной информационной инфраструктуры (при наличии такой инфраструктуры); защиты от вредоносного кода на уровне серверного оборудования; защиты от вредоносного кода на уровне контроля межсетевого трафика; защиты от вредоносного кода на уровне контроля почтового трафика; защиты от вредоносного кода на уровне входного контроля устройств и переносных (отчуждаемых) носителей информации; защиты от вредоносного кода на уровне контроля банкоматов и платежных терминалов для предотвращения несанкционированного получения информации, необходимой для осуществления переводов денежных средств;

2) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают функционирование средств защиты от вредоносного кода: в постоянном, автоматическом режиме, в том числе в части установки их обновлений и сигнатурных баз данных; на АРМ пользователей и эксплуатационного персонала в резидентном режиме, их автоматический запуск при загрузке операционной системы;

3) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают: применение средств защиты от вредоносного кода, реализующих функцию контроля целостности их программных компонентов; контроля отключения и своевременного обновления средств защиты от вредоносного кода; выполнение еженедельных полных проверок на отсутствие вредоносного кода на объектах информационной инфраструктуры; использование средств защиты от вредоносного кода различных производителей как минимум для уровней физических АРМ пользователей и эксплуатационного персонала, серверного оборудования, контроля межсетевого трафика; запрет неконтролируемого открытия самораспаковывающихся архивов и исполняемых файлов, полученных из сети Интернет;

4) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают выполнение проверок на отсутствие вредоносного кода: путем анализа информационных потоков между сегментами контуров безопасности (при наличии более одного контура безопасности) и иными внутренними вычислительными сетями Участника, Агента, Оператора услуг Платежной Инфраструктуры (при наличии); путем анализа информационных потоков между внутренними вычислительными сетями и сетью Интернет; путем анализа информационных потоков между сегментами, предназначенными для размещения банкоматов и платежных терминалов, и сетью Интернет;

5) Участник, Агент, Оператор Услуг Платежной Инфраструктуры, при наличии технической возможности, обеспечивают выполнение предварительных проверок на отсутствие вредоносного кода устанавливаемого или изменяемого программного обеспечения, а также выполнение проверки после установки и (или) изменения программного обеспечения;

6) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают регистрацию: операций по проведению проверок на отсутствие вредоносного кода; фактов выявления вредоносного кода; неконтролируемого использования технологии мобильного кода; сбоев в функционировании средств защиты от вредоносного кода; сбоев в выполнении контроля (проверок) на отсутствие вредоносного кода; отключения средств защиты от вредоносного кода; нарушения целостности программных компонентов средств защиты от вредоносного кода;

7) Участник обеспечивает формирование для клиентов рекомендаций по защите информации от воздействия вредоносного кода.

8) В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Участник, Агент, Оператор, Оператор Услуг Платежной Инфраструктуры обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий

воздействия вредоносного кода.

9) Участник, Агент, Оператор, Оператор Услуг Платежной Инфраструктуры приостанавливают при необходимости осуществление переводов денежных средств на период устранения последствий заражения вредоносным кодом.

10) В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают информирование Оператора в срок, не превышающий 24 часа с момента обнаружения факта воздействия вредоносного кода и о действиях, предпринятых для ликвидации последствий такого воздействия;

11) В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Оператор обеспечивает информирование Участников, Агентов и Операторов Услуг Платежной Инфраструктуры в срок, не превышающий 24 часа с момента обнаружения факта воздействия вредоносного кода и о действиях, предпринятых для ликвидации последствий такого воздействия;

8.9 Состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации при использовании сети Интернет при осуществлении переводов денежных средств

В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации при использовании сети Интернет при осуществлении переводов денежных средств, включаются следующие требования:

1) При использовании сети Интернет для осуществления переводов денежных средств Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают:

i) применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения доступа к содержанию защищаемой информации, передаваемой по сети Интернет;

ii) применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации на объектах информационной инфраструктуры с использованием сети Интернет;

iii) применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения несанкционированного доступа к защищаемой информации путем использования уязвимостей программного обеспечения;

iv) снижение тяжести последствий от воздействий на объекты информационной инфраструктуры с целью создания условий для невозможности предоставления услуг по переводу денежных средств или несвоевременности осуществления переводов денежных средств;

v) фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет.

2) Участник обеспечивает формирование для клиентов рекомендаций по защите информации от несанкционированного доступа путем использования ложных (фальсифицированных) ресурсов сети Интернет.

8.10 Защита информации при осуществлении переводов денежных средств с использованием СКЗИ

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

1) Работы по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом Федеральной службы безопасности Российской Федерации от 9 февраля 2005 года № 66, зарегистрированным Министерством юстиции Российской Федерации 3 марта 2005 года N 6382, 25 мая 2010 года N 17350 («Бюллетень нормативных актов федеральных органов исполнительной власти» от 14 марта 2005 года N 11, от 14 июня 2010 года № 24), и технической документацией на СКЗИ.

2) В случае если Участник, Агент, Оператор Услуг Платежной Инфраструктуры применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа.

3) Участник, Агент, Оператор Услуг Платежной Инфраструктуры применяют СКЗИ, которые:

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

ii) поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;

iii) поддерживают непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

4) В случае применения СКЗИ Участник, Агент, Оператор Услуг Платежной Инфраструктуры определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий:

i) порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления переводов денежных средств;

ii) порядок эксплуатации СКЗИ;

iii) порядок восстановления работоспособности СКЗИ в случаях сбоев и (или) отказов в их работе; порядок внесения изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ;

iv) порядок снятия с эксплуатации СКЗИ;

v) порядок управления ключевой системой;

vi) порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей.

5) Криптографические ключи изготавливаются клиентом (самостоятельно), Оператором Услуг Платежной Инфраструктуры и (или) Участником.

6) Безопасность процессов изготовления криптографических ключей СКЗИ обеспечивается комплексом технологических мер защиты информации, организационных мер защиты информации и технических средств защиты информации в соответствии с технической документацией на СКЗИ.

7) Оператор определяет необходимость использования СКЗИ, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации.

8.11 Состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации с использованием технологических мер защиты информации

В состав требований к обеспечению защиты информации при осуществлении переводов денежных средств, применяемых для защиты информации с использованием технологических мер защиты информации, включаются следующие требования:

1) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают учет и контроль состава, установленного и (или) используемого на средствах вычислительной техники программного обеспечения.

2) Оператор определяет порядок применения организационных мер защиты информации и (или) использования технических средств защиты информации, используемых при проведении операций обмена электронными сообщениями и другой информацией при осуществлении переводов денежных средств. Участник и Оператор Услуг Платежной Инфраструктуры обеспечивают выполнение указанного порядка.

3) Распоряжение клиента, распоряжение Участника и распоряжение ЦПКК в электронном виде может быть удостоверено электронной подписью, а также в соответствии с пунктом 4 статьи 847 Гражданского кодекса Российской Федерации аналогами собственноручной подписи, кодами, паролями и иными средствами, позволяющими подтвердить составление распоряжения уполномоченным на это лицом.

4) При эксплуатации объектов информационной инфраструктуры Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают:

i) защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации;

ii) контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры;

iii) аутентификацию входных электронных сообщений;

iv) взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями; восстановление информации об остатках денежных средств на банковских счетах и данных держателей платежных карт в случае умышленного (случайного) разрушения (искажения) или выхода из строя средств вычислительной техники;

v) сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчетов в Платежной Системе;

vi) выявление фальсифицированных электронных сообщений, в том числе осуществление операций, связанных с осуществлением переводов денежных средств, злоумышленником от имени авторизованного клиента (подмена авторизованного клиента) после выполнения процедуры авторизации.

8.12 Состав требований к обеспечению защиты среды виртуализации при осуществлении переводов денежных средств

В состав требований к обеспечению защиты среды виртуализации при осуществлении переводов денежных средств, включаются следующие требования:

1) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают разграничение и контроль осуществления одновременного доступа к виртуальным машинам с АРМ пользователей и эксплуатационного персонала только в пределах одного контура безопасности (при наличии более одного контура безопасности);

2) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают разграничение и контроль осуществления одновременного доступа виртуальных машин к системе хранения данных в пределах контура безопасности;

3) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают идентификацию и аутентификацию пользователей серверными компонентами виртуализации и (или) средствами централизованных сервисов аутентификации при предоставлении доступа к виртуальным машинам;

4) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают возможность принудительной блокировки (выключения) установленной сессии работы пользователя с виртуальной машиной;

5) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают: контроль и протоколирование доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных с реализацией двухфакторной аутентификации; размещение средств защиты информации, используемых для организации контроля и протоколирования доступа эксплуатационного персонала к серверным компонентам виртуализации и системе хранения данных на физических СВТ; размещение серверных и пользовательских компонентов объектов информационной инфраструктуры на разных виртуальных машинах;

6) В случае наличия более одного контура безопасности Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают: выделение в вычислительных сетях отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения серверных компонент объектов

информационной инфраструктуры, включенных в разные контуры безопасности; выделение в вычислительных сетях отдельных сегментов (групп сегментов), в том числе виртуальных, используемых для размещения совокупности виртуальных машин, предназначенных для размещения АРМ пользователей и эксплуатационного персонала, включенных в разные контуры безопасности; организацию межсетевого экранирования вышеуказанных сегментов (групп сегментов) вычислительных сетей, включая фильтрацию данных на сетевом и прикладном уровнях; реализацию контроля информационного взаимодействия между вышеуказанными сегментами (группами сегментов) вычислительных сетей в соответствии с установленными правилами и протоколами сетевого взаимодействия;

7) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают: регламентацию и контроль выполнения операций в рамках жизненного цикла базовых образов виртуальных машин и операций по копированию образов виртуальных машин; включение в базовые образы виртуальных машин только программного обеспечения технических мер защиты информации, применяемых в пределах виртуальных машин и программного обеспечения автоматизированных систем; отнесение каждой из виртуальных машин только к одному из контуров безопасности; запрет на копирование текущих образов виртуальных машин, использующих СКЗИ, с загруженными криптографическими ключами; контроль завершения сеанса работы пользователей с виртуальными машинами;

8) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают регистрацию операций, связанных с: запуском (остановкой) виртуальных машин; изменением параметров настроек виртуальных сетевых сегментов, реализованных средствами гипервизора; созданием и удалением виртуальных машин; созданием, изменением, копированием, удалением базовых образов виртуальных машин; копированием текущих образов виртуальных машин; изменением прав логического доступа к серверным компонентам виртуализации; изменением параметров настроек серверных компонентов виртуализации; аутентификацией и авторизацией эксплуатационного персонала при осуществлении доступа к серверным компонентам виртуализации; аутентификацией и авторизацией пользователей при осуществлении доступа к виртуальным машинам; параметров настроек технических средств защиты информации, используемых для реализации контроля доступа к серверным компонентам виртуализации; изменением настроек технических средств защиты информации, используемых для обеспечения защиты виртуальных машин;

8.13 Состав требований к повышению осведомленности в области обеспечения защиты информации

В состав требований к повышению осведомленности в области обеспечения защиты информации включаются следующие требования:

1) Участник, Агент, являющийся юридическим лицом, Оператор Услуг Платежной Инфраструктуры обеспечивают повышение осведомленности работников в области обеспечения защиты информации:

i) по порядку применения организационных мер защиты информации;

ii) по порядку использования технических средств защиты информации.

1) Участник, Агент, являющийся юридическим лицом, Оператор Услуг Платежной Инфраструктуры обеспечивают повышение осведомленности работников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации.

2) Участник обеспечивает доведение до клиентов информации о возможных рисках получения несанкционированного доступа к защищаемой информации с целью осуществления переводов денежных средств лицами, не обладающими правом распоряжения этими денежными средствами, и рекомендуемых мерах по их снижению.

8.14 Состав требований к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и реагирования на них и восстановлению штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации, а также мероприятий

по реализации взаимодействия при обмене информацией об инцидентах

В состав требований к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств (далее – инциденты защиты информации), и реагирования на них включаются следующие требования:

1) Оператор определяет:

i) требования к порядку, форме и срокам информирования Оператора, Участников и Операторов Услуг Платежной Инфраструктуры о выявленных в Платежной Системе инцидентах защиты информации; информирование Оператора о выявленных Участниками и Операторами Услуг Платежной Инфраструктуры, привлекаемыми для оказания Услуг Платежной Инфраструктуры в Платежной Системе инцидентах защиты информации при осуществлении переводов денежных средств, осуществляется ежеквартально;

ii) требования к взаимодействию Оператора, Участников и Операторов Услуг Платежной Инфраструктуры в случае выявления инцидентов защиты информации;

2) Участник и Оператор Услуг Платежной Инфраструктуры обеспечивают выполнение указанных в настоящем подпункте требований.

3) Оператор обеспечивает учет и доступность для Участников и Операторов Услуг Платежной Инфраструктуры, привлекаемых для оказания Услуг Платежной Инфраструктуры в Платежной Системе, информации:

i) о выявленных в Платежной Системе инцидентах защиты информации;

ii) о методиках анализа и реагирования на инциденты защиты информации.

4) Участник, Оператор Услуг Платежной Инфраструктуры обеспечивает: установление и применение единых правил реагирования на инциденты защиты информации; создание Группы реагирования на инциденты защиты информации; проведение мероприятий по реагированию на каждый обнаруженный инцидент защиты информации;

8.14.1. Порядок взаимодействия субъектов Платежной Системы в случае выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, и порядок, форма и сроки информирования об инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств

1) Операторы по переводу денежных средств, являющиеся Участниками, и Операторы Услуг Платежной Инфраструктуры должны обеспечить взаимодействие при обмене информацией об инцидентах защиты информации.

2) в случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе не несущего финансовых последствий, но затрагивающего технологические участки, Операторы Услуг Платежной Инфраструктуры, Агенты, Участники должны в срок не позднее 24 часов с момента возникновения (выявления) инцидента, а также в течение 24 часов после его устранения, сообщить о нём в доступной форме в Службу информационной безопасности Оператора. В сообщении об инциденте необходимо указать:

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

3) в случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе несущего финансовые последствия, Операторы Услуг Платежной Инфраструктуры, Участники, Агенты должны незамедлительно, но не позднее одного часа с момента выявления инцидента, сообщить о нём в доступной форме Оператору. В сообщении об инциденте необходимо указать:

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

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

4) Служба информационной безопасности Оператора незамедлительно, но не позднее одного часа с момента выявления инцидента, инициирует информирование Участников и Операторов Услуг Платежной Инфраструктуры в доступной форме по предоставленным ими контактным данным о выявлении инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, который оказывает (или может оказать) влияние на работу соответствующего Участника или соответствующего Оператора Услуг Платежной Инфраструктуры.

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

5) Далее Оператор проводит анализ предоставленных данных, в случае подтверждения реализует комплекс мер, направленных на устранение последствий инцидента, причин, вызвавших инцидент, и на недопущение его повторного возникновения, при необходимости направляет соответствующее уведомление тому субъекту Платежной Системы, в функциональной зоне ответственности которого находится область возникновения инцидента для принятия незамедлительных мер.

6) Субъект Платежной Системы, допустивший инцидент, реализует комплекс мер, направленных на восстановление штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации, а также на устранение последствий инцидента, причин, вызвавших инцидент, и на недопущение его повторного возникновения.

7) Для восстановления штатного функционирования объекта информационной инфраструктуры в случае реализации инцидентов защиты информации субъект Платежной Системы должен иметь внутренние документы по восстановлению штатного функционирования объектов информационной инфраструктуры, которые должны предусматривать последовательные действия, направленные на восстановление работоспособности вышедших из строя автоматизированных систем и(или) программного обеспечения в зависимости от причин возникновения инцидента, и в случае реализации инцидента действовать в соответствии с ними.

8) При осуществлении Участниками мероприятий по реализации Участниками взаимодействия при обмене информацией об инцидентах защиты информации, Участники определяют ответственных лиц для взаимодействия с Оператором и руководствуются п. 5.6 Правил.

9) При осуществлении Операторами Услуг Платежной Инфраструктуры мероприятий по реализации Операторами Услуг Платежной Инфраструктуры взаимодействия при обмене информацией об инцидентах защиты информации, Операторы Услуг Платежной Инфраструктуры определяют ответственных лиц для взаимодействия с Оператором и предоставляют информацию о своей деятельности с использованием следующих каналов/способов передачи информации:

- электронная почта;
- бумажные носители;
- телефонная связь;
- в устной форме во время личных встреч;
- через иные заранее согласованные Оператором Услуг Платежной Инфраструктуры и Оператором каналы связи.

Адреса электронной почты и номера телефонов для использования Оператором Услуг

Платежной Инфраструктуры в целях взаимодействия и обмена информацией как указано выше предоставляются Оператором до начала работы каждого Оператора Услуг Платежной Инфраструктуры в рамках Платежной Системы. В случае изменения указанных номеров телефонов и адресов электронной почты, Оператор уведомит каждого Оператора Услуг Платежной Инфраструктуры о таких изменениях путем направления уведомления в письменном виде или путем направления информации на адрес электронной почты каждого Оператора Услуг Платежной Инфраструктуры или путем размещения соответствующей информации на сайте Оператора www.omnypay.ru.

8.14.2. Содержание, форма и периодичность предоставления информации, направляемой Операторами Платежной Инфраструктуры, Агентами и Участниками Оператору для целей анализа обеспечения в Платежной Системе защиты информации при осуществлении переводов денежных средств

1) для целей анализа обеспечения в Платежной Системе защиты информации при осуществлении переводов денежных средств и расчета показателей уровня риска информационной безопасности Участники, Агенты и Операторы Услуг Платежной Инфраструктуры направляют в Службу информационной безопасности Оператора посредством электронной почты на ежеквартальной основе не позднее пятнадцатого рабочего дня месяца, следующего за отчетным кварталом, в электронном виде отчета по форме Приложения № 9. При этом, такой отчет предоставляется Оператору исключительно в отношении инцидентов, выявленных при работе в Платежной Системе;

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

8.14.3. Порядок обеспечения Оператором учета и доступности для Участников и Операторов Услуг Платежной Инфраструктуры информации о выявленных в Платежной Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, методиках анализа и реагирования на инциденты

1) Служба информационной безопасности Оператора ведет учет выявленных в Платежной Системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, в соответствии с внутренними процедурами, разработанными Оператором.

2) Оператор обеспечивает доступность информации о выявленных в Платежной Системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, путем направления в электронном виде соответствующей информации Участникам и Операторам Услуг Платежной Инфраструктуры в форме отчета на ежеквартальной основе. В случае отсутствия инцидентов за отчетный период такой отчет не направляется. Кроме того, соответствующая информация предоставляется Участникам и Операторам Услуг Платежной Инфраструктуры по их письменному запросу.

3) Оператор разрабатывает и поддерживает в актуальном состоянии методики анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, с учетом системного анализа актуальных факторов риска возникновения инцидентов, характера и периодичности возникновения инцидентов.

4) Оператор обеспечивает доступность методик анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, путем направления Участникам и Операторам Услуг Платежной Инфраструктуры методик на регулярной основе по мере их обновления. Направление актуальной версии методик анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе, осуществляется не реже одного раза в год.

8.14.4. Состав требований к восстановлению штатного функционирования объектов информационной инфраструктуры в случае реализации инцидентов защиты информации

1) Оператор обеспечивает надлежащее (штатное) функционирование Платежной Системы в соответствии с комплексом мероприятий, предусмотренным Порядком обеспечения БФПС.

2) Участниками и Операторами Услуг Платежной Инфраструктуры самостоятельно разрабатываются Планы обеспечения непрерывности деятельности и восстановления деятельности в том числе в случае реализации инцидентов защиты информации, в соответствии с требованиями настоящих Правил, и определяется порядок осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий реализации инцидентов защиты информации, а также порядок пересмотра и тестирования данных Планов.

3) Оператор, Участники и Операторы Услуг Платежной Инфраструктуры информируют друг друга в электронном виде о возобновлении работоспособности после восстановления штатного функционирования инфраструктуры.

4) Оператор определяет следующие требования к мероприятиям по восстановлению штатного функционирования объектов информационной инфраструктуры Участников и Операторов услуг платежной инфраструктуры, которые должны обеспечивать непрерывность работы в нештатных ситуациях:

i) поддержание актуального перечня объектов информационной инфраструктуры, используемого для работы в Платежной Системе;

ii) наличие резервного оборудования, каналов связи, резервных копий программного обеспечения, средств защиты информации, используемых субъектом для работы в Платежной системе;

iii) регулярное выполнение процедур резервного копирования операций, осуществленных в Платежной системе, с применением средств защиты информации;

iv) наличие конкретных восстановительных решений для соответствующего типа объекта информационной инфраструктуры в зависимости от причины возникновения инцидента защиты информации;

v) предотвращение возникновения нештатных ситуаций в будущем путем поиска и устранения выявленных ошибок функционирования объектов информационной инфраструктуры, а также путем оптимизации используемых объектов информационной инфраструктуры;

vi) обеспечение корректировки рабочей документации на используемые объекты информационной инфраструктуры по результатам проведения анализа возникновения нештатных ситуаций и перечня мероприятий для недопущения повторения нештатных ситуаций в будущем;

vii) регулярное обучение персонала.

8.14.5 Порядок анализа и реагирования на инциденты защиты информации при осуществлении переводов денежных средств

1) Ответственное лицо субъекта Платежной Системы после получения информации о выявленном инциденте защиты информации незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа ответственное лицо проводит проверку наличия в выявленном факте нарушений работников и анализ обстоятельств, приведших к возникновению инцидента защиты информации.

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

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

i) дата и время совершения /возникновения инцидента защиты информации;

ii) тип инцидента защиты информации;

iii) условия и причина возникновения инцидента защиты информации;

iv) вид нарушителя, виновного в совершении инцидента защиты информации

(внутренний/внешний);

v) обстоятельства и мотивы совершения инцидента защиты информации;

vi) требования по обеспечению защиты информации, вследствие нарушения которых возник инцидент защиты информации;

vii) последствия инцидента защиты информации;

viii) действия, необходимые для устранения последствий инцидента защиты информации;

ix) факт обращения в правоохранительные органы;

x) планируемая дата завершения разбирательства по инциденту защиты информации.

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

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

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

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

8.14.6 Мероприятия, проводимые Участниками и Операторами Услуг Платежной Инфраструктуры в рамках реагирования на инциденты защиты информации в случае их реализации

Помимо порядка реагирования на инциденты защиты информации при осуществлении переводов денежных средств, установленного выше, Участники и Операторы Услуг Платежной Инфраструктуры обеспечивают организационные и технические меры для реализации мероприятий в рамках реагирования на инциденты защиты информации в случае их реализации. Конкретный комплекс мероприятий определяется, разрабатывается и внедряется Участниками и Операторами Услуг Платежной Инфраструктуры с учетом следующих требований:

1) Участники и Операторы Услуг Платежной Инфраструктуры в своих внутренних документах должны определять и поддерживать в актуальном состоянии:

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

2) Для целей реагирования на инциденты защиты информации в случае их реализации, Участники и Операторы Услуг Платежной Инфраструктуры должны обеспечить наличие и функционирование аппаратных и программных средств, обеспечивающих возможность реализации мероприятий по реагированию на инциденты защиты информации.

3) Перечень мероприятий по реагированию на инциденты защиты информации Участников и

Операторов Услуг Платежной Инфраструктуры должен включать:

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

8.15 Состав требований к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств

В состав требований к определению и реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств включаются следующие требования:

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

i) состав и порядок применения организационных мер защиты информации;

ii) состав и порядок использования технических средств защиты информации, включая информацию о конфигурации технических средств защиты информации, определяющую параметры их работы;

iii) порядок регистрации и хранения информации на бумажных носителях и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации.

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

i) самостоятельного определения Оператором порядка обеспечения защиты информации при осуществлении переводов денежных средств;

ii) распределения обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств между Оператором, Операторами Услуг Платежной Инфраструктуры, Участниками и Агентами;

3) Оператор, Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают определение порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках распределения обязанностей, установленных оператором платежной системы.

4) Для определения порядка обеспечения защиты информации при осуществлении переводов денежных средств Оператор, Участник, Агент, Оператор Услуг Платежной Инфраструктуры в рамках обязанностей, установленных Оператором, могут использовать:

i) положения национальных стандартов по защите информации, стандартов организаций, в том числе стандартов Банка России, рекомендаций в области стандартизации, в том числе рекомендаций Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании;

ii) положения документов, определяемых международными платежными системами;

iii) результаты анализа рисков при обеспечении защиты информации при осуществлении переводов денежных средств на основе моделей угроз и нарушителей безопасности информации, определенных в национальных стандартах по защите информации, стандартах организаций, в том числе стандартах Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании, или на основе моделей угроз и нарушителей безопасности информации, определенных Оператором, Участником, Оператором Услуг Платежной Инфраструктуры.

5) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств.

6) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают назначение лиц, ответственных за выполнение порядка обеспечения защиты информации при осуществлении переводов денежных средств.

7) Служба информационной безопасности Участника, Агента, Оператора Услуг Платежной Инфраструктуры осуществляет контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств, включая:

i) контроль (мониторинг) применения организационных мер защиты информации;

ii) контроль (мониторинг) использования технических средств защиты информации.

8.16 Состав требований к совершенствованию Оператором, Участником, Агентом, Оператором Услуг Платежной Инфраструктуры защиты информации при осуществлении переводов денежных средств

В состав требований к совершенствованию Оператором, Участником, Агентом, Оператором Услуг Платежной Инфраструктуры защиты информации при осуществлении переводов денежных средств включаются следующие требования:

1) Оператор, Участник, Агент, Оператор Услуг Платежной Инфраструктуры регламентируют пересмотр порядка обеспечения защиты информации при осуществлении переводов денежных средств в рамках обязанностей, установленных Оператором, в связи:

i) с изменениями требований к защите информации, определенных Правилами;

ii) с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе;

2) Участник, Агент, Оператор Услуг Платежной Инфраструктуры регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении переводов денежных средств, в случаях:

i) изменения требований к защите информации, определенных Правилами;

ii) изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе;

iii) изменения порядка обеспечения защиты информации при осуществлении переводов денежных средств;

iv) выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении переводов денежных средств;

v) выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств;

vi) выявления недостатков при проведении оценки соответствия;

vii) на основе результатов проведения мероприятий по обнаружению инцидентов защиты информации и реагированию на них;

viii) изменения целевых показателей величины допустимого остаточного операционного риска;

3) Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают формирование и фиксацию решений о необходимости выполнения корректирующих или превентивных действий, в частности пересмотре применяемых мер защиты информации.

4) Принятие решений Участником, Агентом, Оператором Услуг Платежной Инфраструктуры по совершенствованию защиты информации при осуществлении переводов денежных средств согласуется со службой информационной безопасности.

8.17 Состав требований к оценке выполнения Оператором, Участником, Агентом, Оператором Услуг Платежной Инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств

В состав требований к оценке выполнения Оператором, Агентом, Участником, Оператором Услуг Платежной Инфраструктуры требований к обеспечению защиты информации при осуществлении переводов денежных средств включаются следующие требования:

1) Участник, Оператор, Оператор Услуг Платежной Инфраструктуры обеспечивают проведение оценки соответствия уровням защиты информации в соответствии с национальным стандартом РФ ГОСТ Р 57580.2-2018 (далее – ГОСТ Р 57580.2) при осуществлении переводов денежных средств (далее - оценка соответствия); Оператор, Участник, Оператор Услуг Платежной инфраструктуры должны обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018;

2) Агенты обеспечивают реализацию минимального уровня защиты информации для объектов информационной инфраструктуры и уровень соответствия не ниже третьего в соответствии с ГОСТ Р 57580.2-2018;

3) Оценка соответствия осуществляется Оператором, Участником, Агентом, Оператором Услуг Платежной Инфраструктуры с привлечением сторонних организаций, имеющих лицензию на осуществлении деятельности по технической защите конфиденциальной информации, в соответствии с требованиями законодательства Российской Федерации.

4) Оператор, Участник, Агент, Оператор Услуг Платежной Инфраструктуры обеспечивают проведение оценки соответствия не реже одного раза в два года, а также по требованию Банка России.

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

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

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

Наименование Участника, проводившего оценку;

Сроки проведения оценки;

Наименование сторонней организации, проводившей оценку, в соответствии с требованиями законодательства Российской Федерации;

Таблицу оценок, входящих в отчет по результатам оценки соответствия ЗИ в соответствии с ГОСТ Р 57580.2.

8.18 Состав требований к доведению Участником, Агентом, Оператором Услуг Платежной Инфраструктуры до Оператора информации об обеспечении в Платежной Системе защиты информации при осуществлении переводов денежных средств

В состав требований к доведению Участником, Агентом, Оператором Услуг Платежной Инфраструктуры до Оператора информации об обеспечении в платежной системе защиты информации при осуществлении переводов денежных средств включаются следующие требования:

1) Оператор устанавливает требования к содержанию, форме и периодичности представления информации, направляемой Участниками, Агентами и Операторами Услуг Платежной Инфраструктуры Оператору для целей анализа обеспечения в Платежной Системе защиты информации при осуществлении переводов денежных средств.

2) Участник, Агент и Оператор Услуг Платежной Инфраструктуры обеспечивают

выполнение указанных требований.

3) Информация, направляемая Участниками, Агентами и Операторами Услуг Платежной Инфраструктуры, Оператору для целей анализа обеспечения в Платежной Системе защиты информации при осуществлении переводов денежных средств, включает следующую информацию:

i) о степени выполнения требований к обеспечению защиты информации при осуществлении переводов денежных средств;

ii) о реализации порядка обеспечения защиты информации при осуществлении переводов денежных средств;

iii) о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств;

iv) о результатах проведенных оценок соответствия;

v) о выявленных угрозах и уязвимостях в обеспечении защиты информации при проведении ежегодного тестирования на проникновение и анализ уязвимостей объектов информационной инфраструктуры в соответствии с требованиями законодательства Российской Федерации;

vi) о проведении оценки соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже, чем ОУД 4 в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 15408-3-2013 прикладного программного обеспечения автоматизированных систем и приложений, распространяемых клиентам для совершения действий, непосредственно связанных с осуществлением переводов денежных средств и (или) программного обеспечения, эксплуатируемого на участках, используемых для приема документов, связанны с осуществлением переводов денежных средств, составленных в электронном виде, к исполнению в автоматизированных система и приложения с использованием сети Интернет;

8.19 Состав требований по противодействию осуществлению переводов денежных средств без согласия клиента.

Операторы по переводу денежных средств, являющиеся Участниками, и Операторы Услуг Платежной Инфраструктуры должны реализовать мероприятия по противодействию осуществлению переводов денежных средств без согласия клиента, определенные пунктами 3.2 и 3.4 Указания Банка России от 9 января 2023 года № 6354-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами платежных платформ в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента, форме и порядке получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры, операторами электронных платформ мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента», зарегистрированного Министерством юстиции Российской Федерации 25 мая 2023 года № 73472.

8.19.1. Мероприятия по противодействию осуществлению переводов без согласия клиентов:

8.19.1.1 Оператор при реализации мероприятий по противодействию осуществлению переводов без согласия клиента выполняет следующие действия:

– создает систему выявления и мониторинга переводов денежных средств по противодействию переводов денежных средств без согласия клиентов;

– определяет порядок реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента для Участников.

8.19.1.2 Система выявления и мониторинга переводов денежных средств без согласия клиента Оператора основывается на информации о переводах без согласия клиента. Для получения указанной информации Оператор использует техническую инфраструктуру (автоматизированную систему) Банка России, информация о которой размещается на официальном сайте Банка России в сети «Интернет».

8.19.1.3 Участники обязаны самостоятельно реализовывать мероприятия, направленные на противодействие осуществлению переводов денежных средств без согласия клиентов, а также

незамедлительно (не позднее следующего рабочего дня) информировать Оператора по согласованным каналам связи о выявлении операций, имеющих признаки перевода без согласия клиента, и о предпринятых Участником действиях в отношении указанных операций. При этом, Участник при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента должен:

- выявлять операции по переводу денежных средств, соответствующие признакам осуществления перевода денежных средств без согласия клиента;
- выявлять операции по переводу денежных средств, совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры оператора по переводу денежных средств;
- выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия клиента;
- осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, при их наличии;
- осуществлять сбор сведений об обращении плательщика в правоохранительные органы при их наличии;
- рассматривать случаи и (или) попытки осуществления переводов денежных средств без согласия клиента, вызванные компьютерными атаками, направленные на объекты информационной инфраструктуры участников информационного обмена;
- реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента;
- определять в документах, регламентирующих процедуры управления рисками, процедуры выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента, на основе анализа характера, параметров и объема совершаемых клиентами оператора по переводу денежных средств операций (осуществляемой клиентами деятельности) в соответствии с частью 5.1 статьи 8 Федерального закона N 161-ФЗ;
- реализовывать в отношении клиента - получателя средств, в адрес которого ранее совершались операции по переводу денежных средств без согласия клиента, в случаях, предусмотренных договором банковского счета, ограничения по параметрам операций по осуществлению переводов денежных средств (переводов электронных денежных средств) с использованием платежных карт, а также ограничения на получение наличных денежных средств в банкоматах за одну операцию и (или) за определенный период времени;
- использовать выявленную Участником информацию о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры оператора по переводу денежных средств и (или) его клиентов, применительно к своей инфраструктуре в целях противодействия осуществлению переводов денежных средств без согласия клиента.

8.19.1.3.1. С учетом положений п. 8.19.1.3. мероприятия, направленные на противодействие осуществлению переводов денежных средств без согласия клиентов, реализуемые Участником, должны включать:

- определение сотрудников (подразделений) Участника, ответственных за реализацию мероприятий, направленных на противодействие осуществлению переводов денежных средств без согласия клиентов;
- разработку и введение в действие (а также актуализацию) внутренних документов Участника, регламентирующих перечень мероприятий, направленных на противодействие осуществлению переводов денежных средств без согласия клиентов, и порядок реализации таких мероприятий;
- наличие у Участника достаточных аппаратных и программных средств для обеспечения эффективного противодействия осуществлению переводов денежных средств без согласия клиентов (включая систему мониторинга операций клиентов);

- своевременное обновление и модернизацию аппаратных и программных средств для обеспечения эффективного противодействия осуществлению переводов денежных средств без согласия клиентов;

- регулярное обучение сотрудников Участника по вопросам противодействия осуществлению переводов денежных средств без согласия клиентов;

- проведение мероприятий, направленных на повышение осведомленности клиентов Участника о противодействии осуществлению переводов денежных средств без согласия клиентов;

- определение порядка приостановки операции клиента в случае выявления Участником операции, совершенной без согласия клиента, или наличия в операции признаков операции без согласия клиента;

- определение порядка отказа от совершения операции клиента в случае выявления Участником в операции признаков операции, совершаемой без согласия клиента.

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

8.19.1.5 Операторы Услуг Платежной Инфраструктуры при реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента должны:

– самостоятельно и в полном объеме реализовывать меры по противодействию осуществлению переводов денежных средств без согласия клиента (Участника) в соответствии с порядком, установленным Оператором в настоящем разделе;

– выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия клиента;

– рассматривать случаи и (или) попытки осуществления переводов денежных средств без согласия клиента, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры участников информационного обмена;

– реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры участников информационного обмена и (или) их клиентов, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента;

– использовать информацию о переводах без согласия клиента (Участника) для выявления операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента (Участника);

– осуществлять анализ операций, соответствующих признакам осуществления переводов денежных средств без согласия клиента (Участника), в рамках Платежной системы.

8.19.1.5.1. С учетом положений п. 8.19.1.5. мероприятия, направленные на противодействие осуществлению переводов денежных средств без согласия клиентов (Участников), реализуемые Оператором Услуг Платежной Инфраструктуры, должны включать:

- определение сотрудников (подразделений) Оператора Услуг Платежной Инфраструктуры, ответственных за реализацию мероприятий, направленных на противодействие осуществлению переводов денежных средств без согласия клиентов;

- разработку и введение в действие (а также актуализацию) внутренних документов Оператора Услуг Платежной Инфраструктуры, регламентирующих перечень мероприятий, направленных на противодействие осуществлению переводов денежных средств без согласия клиентов (Участников), и порядок реализации таких мероприятий;

- наличие у Оператора Услуг Платежной Инфраструктуры достаточных аппаратных и программных средств для обеспечения эффективного противодействия осуществлению переводов денежных средств без согласия клиентов (Участников) (включая систему мониторинга операций Участника);

- своевременное обновление и модернизацию аппаратных и программных средств для

обеспечения эффективного противодействия осуществлению переводов денежных средств без согласия клиентов (Участников);

- регулярное обучение сотрудников Оператора Услуг Платежной Инфраструктуры по вопросам противодействия осуществлению переводов денежных средств без согласия клиентов;

- определение порядка приостановки операции клиента (Участника) в случае выявления Оператором Услуг Платежной Инфраструктуры операции, совершенной без согласия клиента, или наличия в операции признаков операции без согласия клиента (Участника);

- определение порядка отказа от совершения операции клиента (Участника) в случае выявления Оператором Услуг Платежной Инфраструктуры в операции признаков операции, совершаемой без согласия клиента (Участника).

8.19.1.6 Участники, Оператор и Операторы Услуг Платежной Инфраструктуры информируют Банк России о переводах без согласия клиентов в случаях и в порядке, предусмотренных Указанием Банка России от 09.01.2023 г. № 6354-У.

8.19.1.7 В целях реализации мероприятий по мониторингу осуществления переводов денежных средств без согласия клиента:

i) Оператор создаёт систему выявления и мониторинга переводов денежных средств без согласия клиента в платежной системе на основе информации о переводах без согласия клиента, предоставляемой субъектами Платежной Системы.

ii) Оператор доводит до субъектов Платежной Системы контактные данные подразделения/лица, ответственного за противодействие осуществлению переводов денежных средств без согласия клиентов;

iii) Система выявления и мониторинга переводов денежных средств без согласия клиента строится на базе специализированных антифрод-решений, которые внедряются Оператором в процессинговом центре платёжной системы. Данные решения содержат свод правил, на основании которых принимается решение о возможности отправки и/или выплаты перевода. Правила учитывают особенности поведения клиента, географию его операции, лимиты по операциям и иные критерии. Правила формируются разработчиком антифрод-решения и/или Оператором.

8.20 Требования к управлению риском информационной безопасности, а также выявлению и идентификации риска информационной безопасности, выявлению и анализу риска информационной безопасности Участником, Оператором Услуг Платежной Инфраструктуры

Для управления риском информационной безопасности в Платежной Системе (далее – риск ИБ) как одним из видов операционного риска, источниками реализации которого являются: недостатки процессов обеспечения защиты информации, в том числе недостатки применяемых технологических мер защиты информации, недостатки прикладного программного обеспечения автоматизированных систем и приложений, а также несоблюдение требований к указанным процессам деятельности Участниками и Операторами услуг платежной инфраструктуры должна обеспечиваться реализация второго уровня защиты информации для объектов информационной инфраструктуры, определенных национальным стандартом Российской Федерации ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер", (далее - ГОСТ Р 57580.1-2017) и уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2018 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия». (далее - ГОСТ Р 57580.2-2018).

Для реализации требований по управлению риском ИБ, выявлению и идентификации риска ИБ субъекты Платежной системы в рамках своих полномочий обязаны:

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

Участники и Операторы услуг платежной инфраструктуры должны выстроить процессы выявления и идентификации риска ИБ в Системе в отношении объектов информационной инфраструктуры Участников, Операторов Услуг Платежной Инфраструктуры, исходя из источников их реализации и причин возникновения. При выполнении мероприятий по выявлению и идентификации риска ИБ в отношении своих объектов информационной инфраструктуры Оператор устанавливает следующие требования к Участникам и Операторам услуг платежной инфраструктуры:

1) определять потенциальные угрозы (риски) в отношении объектов информационной инфраструктуры, используемых Участниками и Операторами услуг платежной инфраструктуры для работы в Платежной Системе;

2) классифицировать риски ИБ в отношении объектов информационной инфраструктуры, используемых Участниками и (или) Операторами услуг платежной инфраструктуры для работы в Платежной системе;

3) для выявления и идентификации Риска ИБ использовать способы, включающие в себя в том числе, но не ограничиваясь: анализ произошедших риск-событий, интервьюирование работников субъекта Платежной Системы, позволяющие установить риски ИБ, оказывающие влияние на работу субъекта в Платежной Системе, анализ документации, полученной в результате внутреннего и внешнего аудита и других источников информации.

При проведении мероприятий по выявлению и идентификации риска ИБ в отношении своих объектов информационной инфраструктуры, используемых при работе в Платежной Системе, субъект Платежной Системы должен руководствоваться положениями нормативных актов Банка России, внутренними документами, регламентирующими управление риском ИБ, и требованиями Оператора.

Участники и Операторы услуг платежной инфраструктуры, в рамках собственной инфраструктуры, обеспечивают выявление Инцидентов ИБ, реагирование на выявленные Инциденты ИБ, устранение причин возникновения Инцидентов ИБ, принятие необходимых мер по снижению негативных последствий Инцидентов ИБ, в случае их реализации, и мер по недопущению повторного возникновения Инцидентов ИБ в соответствии с требованиями законодательства и настоящими Правилами.

Участники и Операторы услуг платежной инфраструктуры информируют Оператора о выявленных Инцидентах ИБ в порядке и сроки, установленные в настоящих Правилах.

Участники и Операторы услуг платежной инфраструктуры должны выявлять и анализировать риски ИБ в Платежной Системе. В целях выявления и анализа Участником, и(или) Оператором услуг платежной инфраструктуры, риска ИБ в Платежной Системе, Оператор устанавливает следующие требования к операторам по переводу денежных средств, являющимся Участниками Системы, и Операторам УПИ:

1) проводить анализ и оценку внешних и внутренних факторов, влияющих на информационную безопасность объектов информационной инфраструктуры и бизнес-процессов, в которых участвует субъект Платежной Системы при осуществлении операций в Платежной системе;

2) идентифицировать риски ИБ, которые могут возникнуть при работе в Платежной системе;

3) разработать и поддерживать в актуальном состоянии классификаторы рисков ИБ, риск-событий, причин возникновения риск-событий. При формировании перечня риск-событий учитывать внутренние документы субъекта Платежной Системы, регламентирующие порядок защиты информации при осуществлении переводов денежных средств, результаты оценки соответствия требованиям безопасности, известные уязвимости на объектах информационной инфраструктуры, используемых для выполнения функциональных обязанностей в Платежной Системе;

4) определить уровни присущего риска ИБ и установить уровень допустимого риска ИБ, выделить значимые риски ИБ, определить вероятность реализации риска ИБ, идентифицированного соответствующим субъектом Платежной Системы, при работе в Платежной системе; определить способы управления Риском ИБ и, по необходимости, актуализировать их;

5) вести мониторинг Рисков ИБ, в том числе уровней остаточных Рисков ИБ, и контролировать их соответствие допустимым уровням Рисков ИБ.

Наряду с указанными требованиями Участники и Операторы услуг платежной инфраструктуры

должны вести базу инцидентов ИБ; своевременно информировать Оператора о реализации риска ИБ у субъекта Платежной Системы или о потенциальной угрозе реализации риска ИБ; предпринимать действия, направленные на минимизацию возможных негативных последствий от реализации у субъекта Платежной Системы риска ИБ при работе в Платежной системе; обеспечивать выполнение требований по защите информации при осуществлении переводов денежных средств.

Уровень риска ИБ оценивается по трем показателям:

1) Числовой итоговой оценке соответствия защиты информации ($R_{ГОСТ}$), проводимой в соответствии с требованиями Положения от 17 августа 2023 г. № 821-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств».

2) Числовой оценке отдельно по Процессам ЗИ в соответствии с ГОСТ Р 57580.2-2018

3) Показателем значимости инцидентов ИБ, определяемом количеством инцидентов и степенью их влияния на Участника, Оператора услуг платежной инфраструктуры и/или Оператора Платежной Системы. Показатель значимости инцидентов ИБ приведен в Таблице 1

Таблица 1. Показатель значимости инцидентов ИБ

Низкий	Инцидентов ИБ за отчетный период не зафиксировано или Выявленные инциденты не оказали влияния на Участника или Оператора услуг платежной инфраструктуры и Оператора Платежной Системы
Средний	Произошел один или несколько инцидентов ИБ, повлиявших на Участника или Оператора услуг платежной инфраструктуры и общая сумма потерь по которым не превышает одного миллиона рублей за отчетный период и/или 1% от уставного капитала Участника/Оператора услуг платежной инфраструктуры.
Высокий	Произошел один или несколько инцидентов ИБ, повлиявших на Участника или Оператора платежной инфраструктуры и Оператора Платежной Системы и общая сумма потерь по которым превышает один миллион рублей за отчетный период и/или 1% от уставного капитала Участника/Оператора услуг платежной инфраструктуры.

Таблица 2. Общий показатель уровня риска

Низкий уровень риска	Итоговый уровень соответствия защиты информации – 4 и показатель значимости инцидентов ИБ не превышает низкий.
Средний уровень риска	Итоговый уровень соответствия защиты информации – 3, но при этом не менее 4 процессов ЗИ имеют 4 уровень соответствия защиты информации, а остальные процессы ЗИ имеют уровень не

	ниже 3. Итоговый уровень соответствия защиты информации – 4 и показатель значимости инцидентов ИБ не превышает средний
Высокий уровень риска	Итоговый уровень соответствия защиты информации – 2 и ниже или 1 и более процессов имеют уровень соответствия защиты информации 2 и ниже, при этом итоговый уровень соответствия ЗИ не важен. Показатель значимости инцидентов ИБ высокий

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

Ограничения могут быть сняты по решению Оператора:

- при условии отсутствия инцидентов ИБ в последующие три месяца;
- при условии предоставления документов и информации об устранении причин возникновения инцидентов;
- при условии возмещения убытка Оператору Системы оператором по переводу денежных средств, являющимся Участником, Оператором Услуг Платежной Инфраструктуры.

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

Глава 9. Система управления рисками в Платежной Системе

9.1 Общие положения

9.1.1 Под системой управления рисками (далее «**СУР**») в Платежной Системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для бесперебойности функционирования Платежной Системы (далее «**БФПС**») с учетом размера причиняемого ущерба. БФПС является комплексным свойством Платежной Системы, обозначающим ее способность предупреждать нарушения требований законодательства, Правил, заключенных договоров при взаимодействии субъектов Платежной Системы, а также восстанавливать надлежащее функционирование Платежной Системы в случае его нарушения.

9.2 Организационная структура управления рисками, обеспечивающая контроль за выполнением Участниками требований к управлению рисками, установленных настоящими Правилами

9.2.1 В качестве организационной модели управления рисками в Системе принята модель распределения функций по оценке и управлению рисками между Оператором, Операторами УПИ и Участниками. Оператор определяет требования к функционированию Участников и Операторов УПИ, выполнение которых обеспечивает бесперебойность функционирования Системы в целом. Оператор непосредственно осуществляет координацию деятельности субъектов Системы, направленной на

достижение, подтверждение и поддержание допустимого уровня рисков нарушения БФПС, под которыми понимается присущие функционированию Системы типичные возможности неоказания, ненадлежащего оказания услуг Системы Участникам вследствие наступления неблагоприятных событий, связанных с внутренними и внешними факторами функционирования Системы. Оператор осуществляет координацию деятельности субъектов по обеспечению БФПС в следующем порядке:

Правила устанавливают основные требования к деятельности субъектов Платежной Системы по обеспечению БФПС и реализации ими мероприятий системы управления рисками;

Субъекты Платежной Системы обязаны выполнять, реализовать установленные мероприятия в рамках собственной системы управления рисками, руководствуясь требованиями настоящих Правил.

Оператор контролирует исполнение настоящих Правил, в том числе:

- устанавливает порядок информационного взаимодействия для управления рисками;
- осуществляет постоянное взаимодействие с представителями субъектов Платежной Системы.

9.2.2 Информационные бюллетени, методологические рекомендации и (или) изменения в настоящие Правила Системы по управлению рисками публикуются Оператором по мере выпуска и (или) необходимости на сайте Системы.

9.2.3 Оператор определяет формы осуществления контроля за соблюдением субъектами порядка обеспечения БФПС.

9.2.4 Оператор осуществляет контроль за соблюдением субъектами порядка обеспечения БФПС путем:

анализа предоставляемой субъектами информации в соответствии с порядком доведения до органов управления Оператора соответствующей информации о рисках, установленным настоящими Правилами;

анализа полученных заявлений, обращений и жалоб клиентов и/или субъектов Системы.

9.2.5 Оператор определяет собственную структуру управления рисками и функциональные обязанности лиц и соответствующих структурных подразделений, ответственных за управление рисками. Оператор вправе передать функции по оценке и управлению рисками полностью или частично Расчетному Центру. В случае принятия такого решения, Оператор уведомляет о нем Операторов Услуг Платежной Инфраструктуры и Участников. Такое уведомление должно содержать дату передачи функций и объем передаваемых функций. С даты передачи соответствующих функций, положения настоящих Правил в части выполнения Оператором функций по оценке и управлению рисками применяются к РЦ (с учетом объема передаваемых функций, указанных в уведомлении).

9.2.6 По осуществлению управления рисками устанавливается разграничение ответственности и полномочий между субъектами Платежной Системы.

9.2.6.1 Оператор:

- координирует деятельность субъектов Системы по обеспечению БФПС;
- разрабатывает внутренние документы по управлению рисками в Системе и доводит их до сведения субъектов;
- определяет мероприятия по управлению рисками;
- определяет и внедряет способы управления рисками, включая риски ИБ;
- определяет показатели БФПС в составе ключевых индикаторов риска (далее «КИР»);
- осуществляет анализ рисков нарушения БФПС на основании первичной информации, предоставляемой субъектами;
- устанавливает допустимый уровень рисков нарушения БФПС;
- контролирует соблюдение субъектами Системы порядка обеспечения БФПС и других регламентов, указанных в пункте 2.19 Порядка обеспечения БФПС;
- выявляет текущие изменения присущего уровня риска нарушения БФПС;
- принимает меры, необходимые для достижения или поддержания допустимого уровня рисков нарушения БФПС;
- организует сбор и обработку сведений, используемых для расчета КИР;
- осуществляет информационное взаимодействие с субъектами Системы в целях

управления рисками нарушения БФПС.

9.2.6.2 Операционный центр:

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

9.2.6.3 ЦПКК (ПЦ):

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

9.2.6.4 Расчетный центр:

- уполномочен и несет ответственность за управление операционным риском Платежной Системы в части оказания расчетных услуг;
- уполномочен и несет ответственность за управление расчетным риском (кредитным риском и риском ликвидности), в том числе создает организационную структуру управления кредитным риском и риском ликвидности, а также разрабатывает внутренние нормативные документы, включая методики анализа кредитного риска Платежной Системы и риска ликвидности Платежной Системы в соответствии с условиями настоящих Правил;
- обеспечивает снижение риска нарушения БФПС исключением задержек времени проведения расчетов с Участниками, возникших по вине РЦ.

9.2.6.5 Участники:

- осуществляют соблюдение настоящих Правил, заключенных договоров, законодательства Российской Федерации;
- обеспечивают надлежащую защиту информации;
- обеспечивают поддержание необходимого остатка денежных средств на своих счетах в Расчетном центре.

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

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

9.2.9 Оценка эффективности системы управления рисками проводится Оператором на основании результатов мониторинга риска БФПС и построения профилей рисков, с применением метода экспертных оценок, индекса рисков и элементов методик, основанных на статистическом и сценарном анализе функционирования системы.

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

9.2.11 В качестве экспертов выступают специалисты Оператора, привлеченные специалисты субъектов Системы, также могут привлекаться внешние эксперты.

9.2.12 В случае признания системы управления рисками эффективной, мероприятия по

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

9.2.13 Оператор обеспечивает проведение оценки системы управления рисками в Платежной системе, в том числе используемых методов оценки рисков в Платежной системе, результатов применения способов управления рисками в Платежной системе, не реже одного раза в три года и документально оформляет результаты указанной оценки.

9.2.14 Оператор вносит изменения в систему управления рисками в Платежной системе, в случае если действующая система управления рисками в Платежной системе не обеспечила три и более раза в течение календарного года возможность восстановления оказания Услуг Платежной Инфраструктуры в течение периодов времени, установленных Оператором в п. 1.26.1 Порядка обеспечения БФПС, при их приостановлении.

9.2.15 Оператор при управлении рисками в Платежной системе оценивает риски, возникающие в связи с привлечением поставщиков (провайдеров), предоставляющих услуги в сфере информационных технологий в целях оказания ОУПИ услуг платежной инфраструктуры и (или) предоставляющих услуги обмена информацией при осуществлении операций с использованием электронных средств платежа между операторами по переводу денежных средств и их клиентами и (или) между операторами по переводу денежных средств и иностранными поставщиками платежных услуг, предусмотренные законодательством (далее - поставщики услуг), в том числе обусловленные вероятностью невыполнения поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг.

9.2.16 Оператор обеспечивает хранение сведений по Системе и сведений об инцидентах не менее пяти лет с даты получения указанных сведений.

9.3 Мероприятия системы управления рисками

9.3.1 Система управления рисками в Системе предусматривает выполнение следующих мероприятий:

определение организационной структуры управления рисками, обеспечивающей контроль за выполнением субъектами требований к управлению рисками, установленных настоящими Правилами;

определение мероприятий по управлению риском ИБ в Платежной системе для, а также определение требований к обеспечению защиты информации для процессов, предусмотренных в разделе 8 Правил;

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

доведение до органов управления Оператора Системы соответствующей информации о рисках;

определение показателей БФПС в соответствии с требованиями нормативных актов Банка России;

определение порядка обеспечения БФПС в соответствии с требованиями нормативных актов Банка России;

определение методик анализа рисков в Системе, включая профили рисков, в соответствии с требованиями нормативных актов Банка России;

определение порядка обмена информацией, необходимой для управления рисками;

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

определение порядка изменения операционных и технологических средств и процедур;

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

определение порядка обеспечения защиты информации в Системе.

9.4 Способы управления рисками

9.4.1 Оператор определяет способы управления рисками в Системе, исходя из способов управления рисками, предусмотренных законодательством (далее - способы управления рисками в Платежной системе).

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

9.4.3 Основные способы управления рисками в Платежной Системе, определены в пункте 3 Приложения №4 к Порядку обеспечения БФПС.

9.5 Доведение до органов управления Оператора соответствующей информации о рисках

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

9.5.2 Консолидированная информация об уровне рисков доводится до сведения органов управления Оператора сотрудником, ответственным за управление рисками, по результатам оценки рисков с использованием методик анализа рисков в Системе, включая профили рисков. Информирование об общем уровне рисков в Системе происходит по окончании плановой оценки всех рисков либо внеплановой оценки всех и (или) отдельных рисков в Системе в виде письменных отчетов сотрудника, ответственного за управление рисками, Генеральному директору Оператора.

9.6 Порядок обеспечения бесперебойности функционирования Платежной Системы, показатели бесперебойности функционирования Платежной Системы и методики анализа рисков в Платежной Системе, включая профили рисков

9.6.1 Порядок обеспечения бесперебойности функционирования Платежной Системы, показатели бесперебойности функционирования Платежной Системы и методики анализа рисков в Платежной Системе, включая профили рисков, отражены в Порядке обеспечения бесперебойности функционирования Платежной Системы, являющимся Приложением №3 к настоящим Правилам.

9.7 Порядок обеспечения защиты информации в Платежной Системе

9.7.1 Защита информации в Платежной Системе обеспечивается Оператором и Участниками в соответствии с требованиями законодательства Российской Федерации, Главой 8 настоящих Правил, Приложением № 6 к настоящим Правилам, условиями Оферты, договорами между Участниками и Оператором.

9.8 Порядок обмена информацией, необходимой для управления рисками

9.8.1 В целях управления рисками в Платежной Системе Оператор вправе запрашивать и получать от Участников и Операторов Услуг Платежной Инфраструктуры информацию, необходимую для управления рисками Платежной Системы, а также систематизировать, обрабатывать, накапливать и хранить такую информацию.

Обмен информацией осуществляется с использованием электронной почты или по заранее согласованному каналу связи.

9.8.2 Состав передаваемой информации, а также условия и сроки передачи информации определяются в Порядке обеспечения БФПС и других внутренних документах Оператора, устанавливающих порядок управления рисками.

9.8.3 Участники и Операторы Услуг Платежной Инфраструктуры не вправе необоснованно отказать Оператору в предоставлении информации, указанной в п. 9.7.1. настоящих Правил. В случае если предоставление определенной информации Участниками или Операторами Услуг Платежной Инфраструктуры запрещено в соответствии с законодательством Российской Федерации, Участник или

Оператор Услуг Платежной Инфраструктуры отказывает Оператору в предоставлении такой информации с указанием причины отказа и ссылкой на положения соответствующих нормативных актов Российской Федерации.

9.8.4 Обмен информацией, необходимой для управления рисками в Платежной Системе, может осуществляться в порядке, предусмотренной иными положениями настоящих Правил.

9.9 Порядок изменения операционных и технологических средств и процедур

9.9.1 Порядок изменения операционных и технологических средств и процедур устанавливается Оператором в Порядке обеспечения БФПС.

Глава 10. Противодействие легализации (отмыванию) доходов, полученных преступным путем, финансированию терроризма и финансированию распространения оружия массового уничтожения

10.1 Общие положения

10.1.1 Оператор и Операторы Услуг Платежной Инфраструктуры, Участники и Партнеры осуществляют деятельность, направленную на ПОД/ФТ/ФРОМУ в соответствии с законодательством Российской Федерации и внутренними документами, разработанными в соответствии с законодательством Российской Федерации.

10.1.2 В рамках Платежной Системы Участники и Агенты осуществляют деятельность, направленную на ПОД/ФТ/ФРОМУ в соответствии с законодательством Российской Федерации, внутренними документами, разработанными в соответствии с законодательством Российской Федерации.

10.1.3 Оператор вправе устанавливать дополнительные требования по ПОД/ФТ/ФРОМУ для отдельных Участников в зависимости от способа предоставления Участником доступа своим клиентам к Услугам, включая каналы предоставления Услуг Участником (Терминалы самообслуживания, Интернет-банк и т.д.), установленного в Оферте. Такие дополнительные требования включаются Оператором в Оферту.

10.1.4 В целях обеспечения деятельности Оператора, направленной на ПОД/ФТ/ФРОМУ, Оператор осуществляет сбор данных и информации об Участниках в рамках программы «Знай своего клиента» в соответствии с Приложением № 7 к Правилам. Участники обязуются предоставлять Оператору сведения, информацию и документы в соответствии с требованиями Приложения № 7 к Правилам.

10.2 Порядок сопровождения перевода денежных средств сведениями о плательщике в соответствии с требованиями Федерального закона от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» в случае, если они не содержатся в распоряжении Участника Платежной Системы

10.2.1 При отсутствии сведений об отправителе или получателе перевода денежных средств, наличие которых является обязательным в соответствии с законодательством Российской Федерации и законодательством страны назначения перевода денежных средств и(или) Офертой, распоряжение Участника об отправлении такого перевода денежных средств признается несоответствующим установленным требованиям и не принимается к исполнению.

10.2.2 При приеме перевода в обработку Оператор обеспечивает техническую возможность сопровождения перевода денежных средств необходимыми сведениями.

Глава 11. Порядок осуществления контроля за соблюдением Правил и ответственность

11.1 Общие положения

11.1.1 Оператор осуществляет контроль за соблюдением настоящих Правил Участниками и Операторами Услуг Платежной Инфраструктуры путем мониторинга деятельности Субъектов в процессе оказания услуг в рамках Платежной системы, анализа жалоб и обращений Плательщиков и Получателей, а также Субъектов Системы.

11.1.2 Участники обеспечивают контроль за соблюдением настоящих Правил Агентами таких Участников. За нарушение Агентами настоящих Правил в той части, в которой настоящие Правила могут применяться к Агентам, Участник несет ответственность перед Оператором.

11.1.3 Оператор, Участники, Операторы Услуг Платежной Инфраструктуры несут ответственность за несоблюдение настоящих Правил в соответствии с законодательством Российской Федерации, настоящими Правилами и договорами (в случае их наличия) между Участниками и Оператором, между Оператором и Участниками, между Оператором и Операторами Услуг Платежной Инфраструктуры, а также между Операторами Услуг Платежной Инфраструктуры и Участниками.

11.1.4 Субъекты Платежной Системы несут ответственность за действия/бездействие и/или злоупотребления своих сотрудников (в том числе мошеннические действия), допущенные ими при работе в Платежной Системе, и обязуются возместить друг другу ущерб, нанесенный в результате таких действий/бездействия и/или злоупотреблений. Субъект, действия/бездействие и/или злоупотребления сотрудника (в том числе, но не ограничиваясь, мошеннические действия) при работе в Платежной Системе, привели к негативным последствиям, ущербу обязуется возместить другим субъектам Платежной Системы ущерб, нанесенный им в результате этих действий/бездействия и/или злоупотреблений (в том числе, но не ограничиваясь, мошеннических действий), в течение 7 (семи) рабочих дней с даты получения от субъекта Платежной Системы, которому был причинен ущерб, претензии с приложением документов, обосновывающих претензию. Оператор не несет ответственности за наступление неблагоприятных последствий для третьих лиц, возникших в результате неисполнения Участником или исполнения Участником ненадлежащим образом обязательств, предусмотренных настоящими Правилами.

11.2 Способы и порядок осуществления контроля Оператором за соблюдением Правил

11.2.1 Оператор осуществляет контроль за соблюдением Правил Участниками (или Партнерами) следующими способами:

а) рассмотрение обращений, поступивших от отправителей/получателей переводов денежных средств, в отношении действий (бездействий) Участников при оказании Услуг;

б) сбор и обработка информации о деятельности Участника в рамках Платежной Системы в открытых источниках;

в) получение информации о деятельности Участника в рамках Платежной Системы от самого Участника, иных Участников, Операторов Услуг Платежной Инфраструктуры (в случае привлечения сторонних Операторов Платежной Инфраструктуры);

г) организация Оператором проверок Отделений Участника, офисов Агентов, осуществляющих переводы денежных средств в рамках Платежной Системы по договору с Участником;

д) организация Оператором обучения сотрудников Участников;

е) организация Оператором опросов Участников;

ж) организация Оператором рабочих встреч, телеконференций и семинаров с представителями Участников;

з) применение к Участникам санкций, предусмотренных настоящими Правилами.

11.2.2 Оператор вправе проводить выборочные проверки Отделений Участников, офисов Агентов, в том числе с привлечением третьих организаций. Проверка может проводиться по согласованию с Участником. Без согласования с Участником проверка может проводиться в форме сценария «тайный клиент». В рамках сценария «тайный клиент» сотрудники Оператора или привлеченной Оператором организации могут представляться сотрудникам Участника, Агента в

качестве клиентов, задавать вопросы об Услугах, пользоваться Услугами, совершать иные действия, не нарушающие права Участника.

11.2.3 Оператор осуществляет контроль за соблюдением Правил Операторами Услуг Платежной Инфраструктуры (в случае привлечения сторонних Операторов Платежной Инфраструктуры) следующими способами:

а) рассмотрение обращений, поступивших от Участников, в отношении действий (бездействий) Операторов Услуг Платежной Инфраструктуры;

б) сбор и обработка информации о деятельности Оператора Услуг Платежной Инфраструктуры;

в) получение информации о деятельности Оператора Услуг Платежной Инфраструктуры в рамках Платежной Системы от самого Оператора Услуг Платежной Инфраструктуры;

г) применение к Операторам Услуг Платежной Инфраструктуры санкций, предусмотренных настоящими Правилами.

11.2.4. Контроль за соблюдением настоящих Правил (с учетом способов осуществления контроля, указанных выше) осуществляется в следующем порядке:

11.2.4.1. Контроль осуществляется Оператором самостоятельно или с привлечением третьих лиц.

11.2.4.2. Постоянный контроль за соблюдением Субъектами настоящих Правил осуществляется Операторам на ежедневной основе путем мониторинга текущей деятельности Субъектов.

11.2.4.3. Периодический контроль осуществляется Оператором путем анкетирования Субъектов, которое проводится не реже одного раза в 12 месяцев.

11.2.4.4. В случае, если по результатам контроля выявлены случаи нарушения Правил, которые не приводят (не привели) к нарушению БФПС, Оператор:

- доводит до сведения Субъекта информацию о выявленном нарушении в письменной форме с указанием допущенного нарушения и срока, в течение которого такое нарушение должно быть устранено, при этом указанный срок не может быть менее 5 (Пяти) рабочих дней;

- направляет Субъекту рекомендации по устранению выявленного нарушения и рекомендует им представить Оператору программу мероприятий, направленных на устранение нарушения;

- осуществляет контроль за устранением Субъектами выявленного нарушения в установленный в уведомлении срок.

11.2.4.5. В случае, если по результатам контроля выявлены случаи нарушения Правил, которые приводят (привели) к нарушению БФПС, Оператор:

- направляет предписание об устранении нарушения с указанием срока для его устранения, при этом срок для устранения нарушения может быть менее 5 (Пяти) рабочих дней;

- ограничивает оказание операционных услуг.

11.3 Ответственность Оператора

11.3.1 Оператор несет ответственность исключительно за прямой документально подтвержденный ущерб, причиненный Участникам или Операторам Услуг Платежной Инфраструктуры вследствие несоблюдения Оператором настоящих Правил.

11.3.2 Ответственность Оператора перед Операторами Услуг Платежной Инфраструктуры (в случае привлечения сторонних Операторов Услуг Платежной Инфраструктуры), привлеченными Оператором, определяется в соответствии с настоящими Правилами и условиями договоров между такими Операторами Услуг Платежной Инфраструктуры и Оператором в случае их заключения.

11.3.3 Совокупная ответственность Оператора перед каждым Участником или каждым привлеченным Оператором Услуг Платежной Инфраструктуры (в случае привлечения сторонних Операторов Услуг Платежной Инфраструктуры), за исключением случаев, когда причиненный ущерб вызван умышленным нарушением обязательств со стороны Оператора, не может превышать 25 000 000 российских рублей. Установленное настоящим пунктом ограничение не распространяется на расчетные обязательства Оператора.

11.4 Ответственность Участника

11.4.1 Участник несет ответственность перед Оператором:
а) за несоблюдение настоящих Правил;
б) за ущерб, причиненный Участником Оператору;
в) за просроченную задолженность перед ЦПКК.

11.4.2 В случае несоблюдения настоящих Правил Оператор вправе по своему усмотрению применять к Участнику следующие санкции:

а) приостановить участие Участника в Платежной Системе в порядке и случаях, предусмотренных п. 4.10 настоящих Правил;

б) временно, на срок до устранения Участником несоблюдения настоящих Правил и последствий такого несоблюдения, в одностороннем порядке уменьшить ставку вознаграждения, причитающегося Участнику. При этом максимальная величина, на которую Оператор имеет право уменьшить ставку вознаграждения, причитающегося Участнику, не может превышать 25% (двадцать процентов) от действующей ставки вознаграждения Участника.

11.4.3 Участник возместит Оператору или Оператору Услуг Платежной Инфраструктуры любой ущерб, причиненный Участником Оператору или Оператору Услуг Платежной Инфраструктуры.

11.4.4 В случае если в результате неисполнения (ненадлежащего исполнения) Участником своих обязательств образуется просроченная задолженность Участника перед ЦПКК, ЦПКК вправе требовать от Участника уплаты неустойки (пени), рассчитываемой в следующем порядке:

а) по операциям в долларах США неустойка (пеня) начисляется в долларах США из расчета 10% (десяти процентов) годовых на сумму задолженности за весь период, начинающийся с календарного дня, следующего за днем, в который такая задолженность подлежала погашению в соответствии с настоящими Правилами, и заканчивающийся в день фактического погашения задолженности. При этом такая неустойка (пеня) подлежит выплате в рублях по курсу Банка России на день погашения задолженности;

б) по операциям в российских рублях неустойка (пеня) начисляется в рублях из расчета двойной ключевой ставки Банка России на сумму задолженности за весь период, начинающийся с календарного дня, следующего за днем, в который такая задолженность подлежала погашению в соответствии с настоящими Правилами, и заканчивающийся в день фактического погашения задолженности.

11.5 Ответственность Операторов Услуг Платежной Инфраструктуры

11.5.1 Операторы Услуг Платежной Инфраструктуры, привлеченные Оператором (в случае привлечения сторонних Операторов Платежной Инфраструктуры), несут ответственность перед Оператором и Участниками в соответствии с настоящими Правилами и условиями договоров между такими Операторами Услуг Платежной Инфраструктуры и Оператором.

11.6 Обстоятельства непреодолимой силы.

11.6.1 Субъекты Платежной Системы освобождаются от ответственности за неисполнение или ненадлежащее исполнение своих обязательств, если оно явилось следствием непреодолимой силы при условии, что эти обстоятельства непосредственно повлияли на исполнение обязательств. Под непреодолимой силой понимаются чрезвычайные и непредотвратимые обстоятельства, которые невозможно было предвидеть и предотвратить имеющимися в распоряжении нарушившего обязательство субъекта Платежной Системы разумными средствами, в том числе: землетрясения, наводнения, пожары, эпидемии, аварии на транспорте, военные действия, массовые беспорядки и др.

Субъект Платежной Системы, подвергшийся действию обстоятельств непреодолимой силы и оказавшийся вследствие этого не в состоянии выполнить свои обязательства, должен сообщить об этом в течение одного рабочего дня с момента возникновения указанных обстоятельств в устной форме и в течение трех рабочих дней в письменной форме Оператору, в противном случае субъект Платежной Системы, нарушивший обязательство, не вправе ссылаться на обстоятельства непреодолимой силы.

Уведомление должно содержать данные о характере обстоятельств, оценку их влияния на возможность исполнения своих обязательств и срок исполнения обязательств с приложением подтверждения официальных органов о действии обстоятельств непреодолимой силы.

Глава 12. Перечень платежных систем, с которыми осуществляется взаимодействие, и порядок такого взаимодействия

12.1 Система может осуществлять взаимодействие с другими платежными системами на основании заключенных договоров о взаимодействии операторов платежных систем.

В рамках взаимодействия с платежными системами Оператор увеличивает перечень предоставляемых клиентам услуг и увеличивает географию предоставления услуг по осуществлению переводов денежных средств.

12.2. Оператор Системы ведет перечень платежных систем, с которыми осуществляется взаимодействие, поддерживает его в актуальном состоянии. Перечень ведется по форме Приложения №10 к настоящим Правилам.

12.3. Порядок взаимодействия с привлекаемыми платежными системами:

12.3.1. В сети привлеченной платежной системы осуществляется отправка и (или) выплата гклиентам переводов денежных средств без открытия счета;

12.3.2. В сети Системы осуществляется отправка и (или) выплата клиентам переводов денежных средств без открытия счета.

12.4. Информационное взаимодействие между Системой и привлеченной платежной системой (ами) (далее – ППС) осуществляется между операторами услуг платежной инфраструктуры в режиме реального времени с использованием защищенного канала связи путем обмена электронными сообщениями установленного формата, удостоверенными электронной подписью отправляющей стороны.

12.5. Расчет платежной клиринговой позиции ППС осуществляется ЦПКК за каждый операционный день на конец операционного дня, являющегося рабочим днем. В случае, если операционный день не является рабочим днем, то расчет платежных клиринговых позиций за такой операционный день будет осуществляться в следующий за ним операционный день, являющийся рабочим днем.

12.7. Расчеты осуществляются с расчетным центром ППС в размере сумм, определенных на нетто основе платежных клиринговых позиций, в соответствующих валютах.

12.8. Положительная платежная клиринговая позиция ППС означает перечисление Расчетным центром денежных средств по платежным реквизитам, указанным в договоре с ППС.

12.9. Отрицательная платежная клиринговая позиция ППС означает перечисление расчетным центром ППС денежных средств по платежным реквизитам на счета Расчетного центра/ЦПКК, указанные в договоре с ППС.

12.10. Информация о конкретном размере комиссионного вознаграждения ППС устанавливается в договоре о взаимодействии.

12.11. Перевод денежных средств, отправленный участником ППС, принимается к исполнению ЦПКК в пределах сумм:

- установленного на ППС Лимита кредитного риска (при условии его установления);
- выплаченных в течение Операционного дня участниками ППС переводов денежных средств.

12.12. Порядок взаимодействия с платежными системами, включая платежный клиринг, и проведения расчетов, определенный в настоящем разделе, относится ко всем ППС, если иной порядок не указан в договоре взаимодействия с конкретной платежной системой.

Глава 13. Порядок взаимодействия в чрезвычайных и нестандартных ситуациях. Порядок разрешения споров

13.1 Порядок взаимодействия в чрезвычайных и нестандартных ситуациях.

13.1.1 В случае выявления в рамках Платежной Системы чрезвычайных ситуаций, в том числе, событий, вызвавших системные сбои, субъекты Платежной Системы, выявившие указанные обстоятельства, незамедлительно предпринимают все зависящие от них действия, направленные на снижение вредных последствий, незамедлительно информируют Оператора и субъекта Платежной Системы, в функциональной зоне ответственности которого находится область возникновения чрезвычайной/нестандартной ситуации или сбоя, по любому из доступных каналов связи, в том числе посредством телефонной связи, по факсу, по электронной почте, о возникшей ситуации, включая информирование о событиях, по их мнению, вызвавших чрезвычайную/нестандартную ситуацию, операционные сбои, об их причинах и последствиях.

13.1.2 Оператор незамедлительно после получения информации о возникновении чрезвычайной/нестандартной ситуации предпринимает действия, направленные на снижение вредных последствий, а также, путем взаимодействия с субъектом Платежной Системы, в функциональной зоне ответственности которого находится область возникновения чрезвычайной ситуации, действия, направленные на выявление и устранение причин возникновения чрезвычайной/нестандартной ситуации, на восстановление нормального режима функционирования Платежной Системы, ликвидации негативных последствий.

13.1.3 После восстановления нормального функционирования Платежной системы Оператор информирует заинтересованных субъектов Платежной Системы о предпринятых действиях и достигнутых результатах.

13.2 Порядок разрешения споров.

13.2.1 Общие положения

13.2.1.1 Все споры и разногласия, возникающие в рамках Платежной Системы между субъектами Платежной Системы, а также между субъектами Платежной Системы и клиентами, должны по возможности разрешаться путем проведения переговоров.

13.2.1.2 Моментом возникновения спора между субъектами Платежной Системы (далее «Стороны спора») является дата направления одной Стороной спора другой Стороне(ам) спора заявления о споре (далее «Заявление о споре») в письменном виде с указанием события (действия/бездействия Стороны(он) спора), являющегося причиной спора, предъявляемых требований и их обоснований, а также сроков и предлагаемой формы проведения переговоров.

13.2.1.3 Моментом возникновения спора между субъектами Платежной Системы и клиентами является дата получения субъектом Платежной Системы претензии клиента.

13.2.1.4 В случае, если Оператор не является Стороной спора, Сторона спора, заявляющая о наличии спора, направляет копию Заявления о споре Оператору для ознакомления одновременно с направлением оригинала(ов) Заявления(ий) о споре другой(им) Стороне(ам) спора.

13.2.1.5 Оператор вправе принимать участие в досудебном разрешении споров и разногласий, возникающих в рамках Платежной Системы между субъектами Платежной Системы , а также между субъектами Платежной Системы и клиентами в соответствии с положениями настоящих Правил.

13.2.2 Досудебное разрешение споров между Участниками и их клиентами в отношении Услуг

13.2.2.1 Досудебное разрешение споров между Участниками и их клиентами в отношении Услуг осуществляется в соответствии с процедурами, установленными Условиями оказания Услуг.

13.2.3 Досудебное разрешение споров между субъектами Платежной Системы

13.2.3.1 Досудебное разрешение споров между субъектами Платежной Системы происходит путем проведения переговоров, в том числе путем обмена письмами, электронными сообщениями, проведением рабочих встреч и совещаний, а также путем совершения иных действий, направленных на

урегулирование спора. Стороны спора вправе привлекать Оператора в качестве третьей стороны (если Оператор не является Стороной спора), не принимающей участия в споре. При этом Оператор вправе высказывать свое мнение относительно спора, знакомиться с фактическими обстоятельствами спора, давать Сторонам спора рекомендации в отношении спора. Мнение Оператора по вопросу спора носит исключительно рекомендательный характер.

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

13.2.3.3 В случае недостижения Сторонами спора соглашения о разрешении спора в досудебном порядке в течение 60 (шестидесяти) дней с даты направления Стороной спора другой Стороне спора Заявления о споре, а также в случае отсутствия таких переговоров в течение того же периода любая из Сторон спора вправе обратиться в суд в соответствии с п. 13.2.4 настоящих Правил.

13.2.4 Подсудность и применимое Право

13.2.4.1 Все споры, разногласия и требования между Участниками и их клиентами, а также между Оператором и клиентами Участников, связанные с оказанием Участниками Услуг, при недостижении сторонами договоренности в соответствии с настоящей Главой 13 в досудебном порядке подлежат разрешению в судах Российской Федерации в соответствии с их подсудностью.

13.2.4.2 Все споры, разногласия или требования между субъектами Платежной Системы, в том числе касающиеся исполнения, нарушения, прекращения или недействительности настоящих Правил и договоров, заключенных между субъектами Платежной Системы в связи с настоящими Правилами, при недостижении договоренности в соответствии с настоящей Главой 13 в досудебном порядке подлежат разрешению в Арбитражном суде города Москвы.

13.2.4.3 Настоящие Правила составлены и подлежат истолкованию в соответствии с законодательством Российской Федерации.

Глава 14. Порядок вступления в силу и внесения изменений в Правила

14.1 Настоящие Правила вступают в силу со дня получения Оператором регистрационного свидетельства Банка России в соответствии с требованиями Федерального закона № 161-ФЗ от 27.06.2011г. «О национальной платежной системе».

14.2 Настоящие Правила являются обязательными для исполнения всеми субъектами Платежной Системы.

14.3 Оператор имеет право в одностороннем порядке вносить изменения в Правила при соблюдении следующих условий:

14.3.1. В случае, если изменения в Правила не приводят к увеличению действующих тарифов или введению новых тарифов при условии:

а) обеспечения Участникам возможности предварительного ознакомления с предлагаемыми изменениями и направления своего мнения Оператору в установленный им срок, который не может быть менее одного месяца с даты обеспечения Участникам возможности предварительного ознакомления с предлагаемыми изменениями;

б) установления срока внесения изменений не менее одного месяца со дня окончания срока, указанного выше.

14.3.2. В случае, если изменения в Правила приводят к увеличению действующих тарифов (или Платы за перевод) или к введению новых тарифов (или Платы за перевод) при условии:

а) уведомления Банка России в срок не менее чем за 30 (тридцать) календарных дней до дня введения в действие изменений в Правила с предоставлением обоснования указанных изменений;

б) обеспечения Участникам возможности предварительного ознакомления с предлагаемыми изменениями и направления своего мнения Оператору в установленный им срок, который не может

быть менее одного месяца с даты обеспечения Участникам возможности предварительного ознакомления с предлагаемыми изменениями;

в) установления срока внесения изменений не менее одного месяца со дня окончания срока, указанного выше.

14.4 При принятии решения об изменении Правил Оператор обеспечивает Участникам возможность предварительного ознакомления с предлагаемыми изменения и направления своего мнения Оператору путем размещения проекта Правил на сайте www.omnypay.ru. При этом Оператор направляет Участникам уведомление в электронной форме о размещении проекта Правил на сайте и о сроках для направления своего мнения Оператору и сроках вступления в силу Правил в размещенной редакции. Указанные сроки устанавливаются Оператором с учетом положений п. 14.3 настоящих Правил.

14.5 Оператор предоставляет в Банк России все изменения Правил, а также изменения перечня Операторов Услуг Платежной Инфраструктуры не позднее 10 (десяти) дней со дня внесения соответствующих изменений.

Глава 15. Прочие условия

15.1 Отказ субъекта Платежной Системы от требований, возникающих из нарушения какого-либо положения или условия настоящих Правил, не должен рассматриваться как отказ от требований, возникающих из любого последующего нарушения того же или иного положения или условия.

15.2 Участник не может передать свои права и обязательства, вытекающие из настоящих Правил или связанные с ними, третьим лицам без письменного согласия Оператора.

15.3 В случаях, когда порядок направления уведомлений, запросов, согласований и иных документов, имеющих юридическое значение для отношений субъектов Платежной Системы (далее «Корреспонденция»), прямо не определен настоящими Правилами, такая Корреспонденция должна быть составлена в письменной форме на русском языке и отправлена получателю Корреспонденции по почтовому адресу/адресу или адресу электронной почты, согласованными между получателем и отправителем Корреспонденции. Использование отдельных терминов на английском языке допускается в Корреспонденции в случае, если такие термины определены в настоящих Правилах или непосредственно в Корреспонденции.

15.4 Все приложения к настоящим Правилам составляют их неотъемлемую часть.

15.5 Недействительность отдельных положений настоящих Правил не влечет недействительность Правил в целом. В случае признания отдельных положений настоящих Правил недействительными все иные положения настоящих Правил продолжат действовать в полном объеме.

Приложение № 1
к Правилам Платежной Системы

Форма заявления
на участие в Платежной Системе

Исх. №_____
Дата:_____ 20___ г.

Оператору Платежной Системы _____

От_____
_____
_____
Адрес:_____

Заявление
на участие в Платежной Системе

1. Настоящим _____ (наименование организации) в лице _____ (должность и ФИО уполномоченного представителя Заявителя), действующего(ей) на основании_____ (наименование документа, уполномочивающего представителя Заявителя на подачу данного заявления от имени Заявителя) (далее «Заявитель»), направляет оператору Платежной Системы _____ (далее «Оператор») настоящее заявление на участие в Платежной Системе в качестве Участника.

2. В целях рассмотрения Оператором настоящего заявления и принятия решения о возможности участия Заявителя в Платежной Системе настоящим Заявитель направляет в адрес Оператора документы согласно перечню, указанному в пункте 8 ниже. Заявитель подтверждает полноту и достоверность данных, содержащихся в прилагаемых документах.

3. Заявитель подтверждает, что ознакомился с Правилами Платежной Системы, размещенными на сайте www.omnypay.ru, действующими на дату настоящего заявления, и настоящим заявляет о своем согласии с указанными Правилами.

4. Заявитель понимает и соглашается с тем, что факт получения Оператором настоящего Заявления:

4.1 не влечет автоматического присоединения Заявителя к Платежной Системе;

4.2 не налагает на Оператора каких-либо обязательств направить Заявителю Оферту об участии в Платежной Системе в качестве Участника.

5. Заявитель настоящим обязуется обеспечить конфиденциальность информации, которую Оператор может направить Заявителю в Оферте или предоставить иным образом. Заявитель обязуется не разглашать такую информацию третьим лицам. Заявитель понимает, что разглашение информации, предоставленной Заявителю Оператором после получения настоящего Заявления, является основанием для отзыва Оферты Оператором и взыскания с Заявителя любых убытков и ущерба, причиненных Оператору в результате разглашения Заявителем соответствующей информации.

6. По всем вопросам, связанным с настоящим заявлением, просим обращаться к нашему ответственному сотруднику _____ (ФИО и должность ответственного сотрудника) по телефону_____ или адресу электронной почты_____.

7. Настоящее заявление составлено в одном экземпляре на _____ листах.

8. Перечень прилагаемых документов:
- _____ _____1 экз., на _____ листах
- _____ _____1 экз., на _____ листах

От имени Заявителя:

_____ (должность)
_____(ФИО)
_____(подпись)
М.П.

Приложение № 2
к Правилам Платежной Системы

Форма Оферты

ОФЕРТА
Об участии в Платежной Системе

г. Москва «___»_____ _____ г.

Настоящим _____, зарегистрированное Банком России в качестве оператора Платежной Системы «Омнипэй» (регистрационный №_____) в лице _____, действующего(ей) на основании_____ (далее «Оператор») в связи с рассмотрением заявления об участии в Платежной Системе №_____ от _____ 20_ г., поступившим от _____ (далее «Заявитель»), предлагает Заявителю стать участником Платежной Системы путем присоединения к Правилам и на изложенных ниже условиях настоящей оферты (далее «Оферта»):

1. Все термины, используемые в Оферте с заглавной буквы и не определенные по тексту Оферты, имеют значение, установленное для них в Правилах, действующих на дату настоящей Оферты.

2. Настоящая Оферта составлена в соответствии с процедурой, установленной в п. 4.2 Правил.

3. Вид участия:

3.1 В соответствии с положениями Правил Оператор настоящей Офертой предлагает Заявителю стать Участником.

4. Перечень Услуг, которые будет оказывать Заявитель в качестве Участника своим клиентам в рамках Платежной Системы и формы приема-выдачи денежных средств при оказании Услуг

4.1 Заявителю предлагается оказывать следующие Услуги:
4.1.1 _____
4.1.2_____

4.2 Формы приема и выдачи денежных средств при оказании Услуг:
4.2.1_____
4.2.2_____

5. Способы обеспечения доступа Заявителя к Платежной Системе, предоставления Заявителем доступа своим клиентам к Услугам, включая каналы предоставления Услуг

5.1 Доступ Заявителя к Платежной Системе будет осуществляться следующим образом:
5.1.1_____
5.1.2_____

5.2 Заявитель обеспечит доступ своим клиентам к Услугам следующими способами и через следующие каналы:

5.2.1_____
5.2.2_____

6. В соответствии с п. 5 настоящей Оферты Заявитель обеспечит следующие требования к защите информации:

6.1_____
6.2_____

7. В соответствии с п. 5 настоящей Оферты Заявитель и Оператор заключат следующие договоры до начала фактического осуществления Заявителем переводов денежных средств в Платежной Системе (если применимо):

7.1_____
7.2_____

8. Плата за перевод.

8.1 Размер Платы за перевод, взимаемой Заявителем со своих клиентов, устанавливается в соответствии с Приложением № 5 к Правилам.

9. Ставка вознаграждения Заявителя за оказание Услуг в качестве Участника.

9.1 За оказание Услуг, Заявителю, в качестве Участника будет причитаться следующее вознаграждение:

9.1.1_____

9.1.2_____

10. Для целей расчетов с Заявителем устанавливаются следующие Отчетный период и пороговые величины задолженности Заявителя:

10.1_____

10.2_____

11. Лимиты на отправление переводов денежных средств Заявителем и расчет размера гарантийного взноса:

11.1_____

11.2_____

12. Дополнительные условия сотрудничества, устанавливаемые с учетом особенностей условий настоящей Оферты (если применимо):

12.1_____

12.2_____

13. Изменение условий участия Заявителя в Платежной Системе.

13.1 В случае, если после получения Заявителем статуса Участника в соответствии с условиями, установленными Правилами и настоящей Офертой, Оператор и Заявитель придут к договоренности об изменении условий участия Заявителя в Платежной Системе, установленных в настоящей Оферте, Оператор подготовит и направит Заявителю дополнительную Оферту, составленную по образцу Приложения № 1 к настоящей Оферте.

13.2 Оператор вправе в соответствии с Правилами в одностороннем порядке изменять размер Платы за перевод, пороговые величины задолженности, установленные в п. 10 настоящей Оферты, а также лимиты на отправление переводов денежных средств, установленные в п. 11 настоящей Оферты.

14. Настоящая Оферта действительна в течение _____ (_____) календарных дней с даты, указанной выше.

15. Настоящая Оферта составлена в двух экземплярах, имеющих одинаковую юридическую силу.

16. Любая информация, содержащаяся в настоящей Оферте, является конфиденциальной. После получения настоящей Оферты Заявитель обязуется не разглашать такую конфиденциальную информацию третьим лицам.

17. Для принятия настоящей Оферты Заявитель должен заполнить Акцепт и направить в адрес Оператора один заполненный экземпляр настоящей Оферты с заполненным Акцептом.

От имени Оператора:

_____ (должность)
_____(ФИО)
_____(подпись)
М.П.

Акцепт Заявителя:

1. Настоящим Заявитель подтверждает свое согласие со всеми условиями Оферты, изложенными выше.

2. Настоящим Заявитель подтверждает свое присоединение к Правилам и обязуется соблюдать их в полном объеме с даты Акцепта.

3. Заявитель обязуется перечислить гарантийный взнос (если применимо) в размере, установленном Офертой, в течение ____(_____) календарных дней с даты Акцепта.

От имени Заявителя:

_____ (должность)
_____(ФИО)
_____(подпись)
М.П.

Дата Акцепта:_____ 20___ г.

Приложение № 1 к Оферте от _____

Форма Оферты
об изменении условий участия в Платежной Системе

г. Москва «___»_____ _____ г.
Настоящим _____, зарегистрированное Банком России в качестве оператора Платежной Системы (регистрационный №_____) в лице _____, действующего(ей) на основании_____ (далее «Оператор») в связи с необходимостью изменения условий участия в Платежной Системе _____ (далее «Участник»), установленных в Оферте №_____ от _____, предлагает Участнику изменить следующие условия участия в Платежной Системе :
1. Все термины, используемые в настоящей Оферте с заглавной буквы и не определенные по тексту, имеют значение, определенное для них в действующей редакции Правил.
2. Оператор предлагает изменить следующие условия Оферты № _____ от _____
2.1_____
2.2_____
3. Настоящая Оферта действительна в течение _____ (_____) календарных дней с даты, указанной выше. Акцептуя настоящую Оферту, Участник подтверждает полную техническую готовность для выполнения условий, указанных в настоящей Оферте.
4. Настоящая Оферта составлена в двух экземплярах, имеющих одинаковую юридическую силу.
5. Любая информация, содержащаяся в настоящей Оферте, является конфиденциальной. После получения настоящей Оферты Участник обязуется не разглашать такую конфиденциальную информацию третьим лицам.
6. Для принятия настоящей Оферты Заявитель должен заполнить Акцепт и направить в адрес Оператора один заполненный экземпляр настоящей Оферты с заполненным Акцептом.
7. Условия Оферты № _____ от _____ считаются измененными с даты получения Оператором Акцепта.

От имени Оператора:
_____ (должность)
_____(ФИО)
_____(подпись)
М.П.

Акцепт Участника:

1. Настоящим Участник подтверждает свое согласие со всеми условиями Оферты, изложенными выше.

От имени Участника:
_____ (должность)
_____(ФИО)
_____(подпись)
М.П.

Приложение № 3
к Правилам Платежной Системы

Порядок обеспечения БФПС

1 Управление рисками в Платежной Системе

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

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

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

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

1.5 Инцидент – это риск-событие, которому присвоен соответствующий уровень воздействия на деятельность Платежной Системы по критериям существенности (значимости) риск-событий (Приложение №3 к настоящему Порядку). Инцидент может привести к нарушению оказания УПИ в соответствии с требованиями к оказанию услуг и влиять на БФПС.

1.6 Организационная модель управления рисками определяется в соответствии с Правилами Платежной Системы.

1.7 Обязанности субъектов Платежной Системы по управлению рисками.
1.7.1 Оператор обязан:
1.7.1.1 определить организационную структуру СУР Оператора;
1.7.1.2 обеспечить контроль выполнения Операторами УПИ и Участниками Платежной Системы требований СУР;
1.7.1.3 с учетом выбранной модели управления рисками в Платежной Системе определить методики анализа рисков в Платежной Системе, включая классификацию рисков, методы их выявления и оценки, определение присущих и остаточных уровней рисков и установку допустимых уровней рисков, а также Способов управления рисками с целью снижения их уровней;
1.7.1.4 проводить стресс-тестирование значимых рисков Платежной Системы;
1.7.1.5 осуществлять мероприятия по составлению профиля рисков Платежной Системы;
1.7.1.6 выявлять инциденты на основании положений настоящего Порядка, определять уровни их влияния на деятельность, в том числе нарушение УПИ в соответствии с требованиями к оказанию услуг и влияние на БФПС;
1.7.1.7 определять КИР, устанавливать их пороговые уровни, а также разрабатывать методы их мониторинга и оценки;
1.7.1.8 выполнять расчет и мониторинг значений КИР (в том числе сравнение фактических значений с пороговыми значениями КИР);

1.7.1.9 вносить изменения в СУР;
1.7.1.10 определять порядок обмена информацией между субъектами Платежной Системы, в том числе о риск-событиях (инцидентах) в Платежной Системе;
1.7.1.11 определять порядок действий субъектов Платежной Системы при возникновении спорных, нестандартных и чрезвычайных ситуаций;
1.7.1.12 определять операционные и технологические требования к программно-аппаратным комплексам Платежной Системы и процедурам предоставления услуг Платежной Системы и контролировать их исполнение;
1.7.1.13 определять требования к порядку оценки качества и надежности функционирования информационных систем, операционных и технологических средств субъектов Платежной Системы;
1.7.1.14 определять требования по обеспечению защиты информации в Платежной Системе и контролировать выполнение;
1.7.2 привлекать в качестве Расчетного центра Платежной Системы банки, являющиеся участниками системы обязательного страхования вкладов в банках Российской Федерации, либо небанковские кредитные организации, осуществляющие расчеты по счетам других кредитных организаций не менее трех лет;Операторы УПИ обязаны выполнять требования в отношении оказываемых ими услуг:
1.7.2.1 организовать СУР в соответствии с требованиями законодательства Российской Федерации и нормативными документами Банка России, настоящими Правилами, в том числе настоящим Порядком, обеспечивающую осуществление идентификацию, мониторинга и анализа рисков на постоянной основе;
1.7.2.2 выявлять инциденты с учетом положений настоящего Порядка, уведомлять Оператора в течение 1 часа с момента возникновения (выявления) инцидента в соответствии с настоящим Порядком;
1.7.2.3 соблюдать требования Платежной Системы по безопасности и защите информации;
1.7.2.4 проводить стресс-тестирование значимых рисков в соответствии с требованиями законодательства Российской Федерации и нормативными актами Банка России;
1.7.2.5 проводить на постоянной основе мониторинг, выявление и анализ риск-событий Платежной Системы в соответствии с требованиями законодательства Российской Федерации, нормативными документами Банка России;
1.7.2.6 проводить расчет и мониторинга значений КИР (в том числе сравнении фактических значений с пороговыми значениями КИР) по событиям Оператора УПИ в соответствии с согласованным порядком между Оператором УПИ и Оператором;
1.7.2.7 осуществлять сбор, обработку и систематизацию сведений о функционировании услуг Оператора УПИ в порядке и сроки, указанные в Статье 4 настоящего Порядка;
1.7.2.8 по запросу Оператора в рамках проводимого им анкетирования не реже одного раза в год предоставлять Оператору информацию о риск-событиях;
1.7.2.9 проводить оценку качества операционных и технологических средств и информационных систем в соответствии с требованиями 161-ФЗ и с учетом условий, изложенных в пункте 2.15.1 настоящего Порядка;
1.7.2.10 участвовать в мероприятиях, связанных с идентификацией и оценкой рисков Платежной Системы, включая составление профиля рисков;
1.7.2.11 назначить сотрудника, ответственного за взаимодействие с Оператором по вопросам управления рисками Платежной Системы и обеспечения бесперебойности функционирования Оператора УПИ в Платежной Системе в отношении оказываемых Оператором УПИ услуг.
1.7.3 Участники обязаны:
1.7.3.1 Сообщать Оператору по электронной почте в течение 24 часов с момента выявления:
1.7.3.1.1 о неисполнении или ненадлежащем исполнении своих обязательств;
1.7.3.1.2 о наличии претензий, предписаний от Банка России в отношении их деятельности в качестве Участников;
1.7.3.1.3 о получении претензий от клиентов в отношении их деятельности в качестве Участников;
1.7.3.1.4 о возникновении инцидентов, касающихся переводов денежных средств, осуществленных Участником в рамках Платежной Системы, в соответствии с п.3.3 настоящего Порядка

1.7.3.2 организовать СУР в соответствии с требованиями законодательства Российской Федерации, нормативными документами Банка России и настоящим Порядком.

1.8 Оператор устанавливает уровни оказания УПИ, характеризующие качество функционирования операционных и технологических средств платежной инфраструктуры (Приложение №3 к настоящему Порядку).

1.9 Операторы УПИ обязаны включать в планы действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности Операторов УПИ в случае возникновения нестандартных и чрезвычайных ситуаций мероприятия по переходу на резервный комплекс программных и (или) технических средств Оператора УПИ в случае приостановления оказания УПИ, а также мероприятия, осуществляемые в случае неработоспособности систем и сервисов поставщиков (провайдеров), предоставляющих услуги в сфере информационных технологий в целях оказания Оператором УПИ услуг платежной инфраструктуры и (или) предоставляющих услуги обмена информацией для осуществления операций с использованием электронных денежных средств платежа между операторами по переводу денежных средств и их клиентами и (или) между операторами по переводу денежных средств иностранными поставщиками платежных услуг, предусмотренные пунктом 33 статьи 3 Федерального закона №161-ФЗ (далее – поставщики услуг), нарушение предоставления которых способно привести к приостановлению оказания УПИ.

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

1.11 Идентификация рисков предусматривает выполнение следующих мероприятий не реже одного раза в год:
1.11.1 формирование и поддержание в актуальном состоянии перечня бизнес-процессов;
1.11.2 выявление риск-событий, и определение для каждого из выявленных риск-событий величины риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации;
1.11.3 разработка и поддержка в актуальном состоянии классификаторов рисков в Платежной Системе, риск-событий и причин риск-событий.

1.12 Оценка рисков проводится Оператором с учетом рисков, возникающих в связи с привлечением поставщиков услуг, в том числе обусловленных вероятностью невыполнения поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг. Риски, возникающие в связи с привлечением поставщиков услуг, в том числе обусловленные вероятностью невыполнения поставщиками услуг своих обязательств, включая возникновение отказов и (или) нарушений функционирования автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования поставщиков услуг, идентифицируются в соответствии с пунктом 1.11 настоящего Порядка.

1.13 Оценка рисков в Платежной Системе предусматривает следующие мероприятия:
1.13.1 проведение анализа бизнес-процессов, в том числе анализа программных и (или) технических средств Операторов УПИ, учитывая факт привлечения ими поставщиков услуг, и других факторов, влияющих на БФПС;
1.13.2 формирования перечня риск-событий для каждого бизнес-процесса с указанием причин риск-событий и их последствий;

1.13.3 определение для каждого из выявленных рисков в Платежной системе уровня присущего риска до применения способов управления рисками в Платежной системе и установление уровня допустимого риска, указанного в пункте 1.19.2 настоящего Порядка;
1.13.4 определение значимых рисков в Платежной Системе, указанных в пункте 1.19.3 настоящего Порядка, путем сопоставления уровня присущего риска до применения способов управления рисками в Платежной Системе и уровня допустимого риска, указанного в пункте 1.19.2 настоящего Порядка, по каждому из выявленных рисков в Платежной Системе;
1.13.5 применение способов управления рисками для каждого из значимых рисков в Платежной Системе, указанных в пункте 1.19.3 настоящего Порядка, и последующее определение для них уровня остаточного риска после применения способов управления рисками в Платежной системе с целью определения уровня остаточного риска для каждого из значимых для Платежной Системы рисков;
1.13.6 сопоставление уровней остаточного риска после применения способов управления рисками в Платежной Системе и уровня допустимого риска, указанного в пункте 1.19.2 настоящего Порядка, для каждого из значимых рисков в Платежной Системе, указанных в пункте 1.19.3 настоящего Порядка, и принятие решения о необходимости применения других способов управления рисками в Платежной Системе в дополнение к ранее примененным способами допустимого уровня рисков для каждого из значимых для Платежной Системы рисков для принятия решения о необходимости применения дополнительных способов управления рисками в Платежной Системе.

1.14 Результат идентификации и оценки рисков в Платежной Системе отражается в профилях рисков. Перечень информации, содержащейся в профилях рисков, указан в Приложении №4 к настоящему Порядку.

1.15 Оператор составляет и пересматривает (актуализирует) профиль каждого из значимых рисков в Платежной Системе, указанных в пункте 1.19.3 настоящего Порядка, включая профиль риска нарушения БФПС.

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

1.17 Оператор проводит плановую оценку рисков в Платежной Системе, а также внеплановые оценки рисков в Платежной Системе с использованием методик анализа рисков в Платежной Системе и составлением профилей рисков.

1.18 Оператор проводит внеплановую оценку всех рисков в Платежной Системе при внесении изменений в один или несколько процессов, в рамках которых обеспечивается оказание УПИ (далее – бизнес-процесс), или в несколько бизнес-процессов. Проведение внеплановой оценки всех рисков в Платежной Системе должно быть завершено не позднее истечения шести месяцев со дня внесения указанных изменений.
1.19 Оператор проводит внеплановую оценку рисков (отдельного риска) в Платежной Системе:
1.19.1 при возникновении события, реализация которого привела к приостановлению (прекращению) оказания УПИ и описание которого в профиле рисков не предусмотрено, либо негативные последствия от его реализации превышают негативные последствия, предусмотренные для этого события в профиле риска;
1.19.2 при установлении по результатам проводимого Оператором мониторинга рисков факта приближения фактического уровня риска к уровню допустимого риска, при котором восстановление оказания УПИ, соответствующих требованиям к оказанию услуг, включая восстановление оказания УПИ в случае приостановления их оказания, осуществляется в течение периодов времени, установленных Оператором, и предполагаемый ущерб от которого Оператор готов принять без применения способов управления рисками в Платежной Системе;

1.19.3 при выявлении значимого риска в Платежной Системе, для которого уровень присущего риска до применения способов управления рисками в Платежной Системе может превысить или превысил уровень допустимого риска;
1.19.4 Проведение внеплановой оценки отдельных рисков (отдельного риска) в Платежной Системе должно быть завершено не позднее истечения четырех месяцев со дня возникновения событий, предусмотренных подпунктами 1.19.1 и 1.19.2 настоящего пункта, либо со дня выявления значимого риска в Платежной Системе, указанного подпункте 1.19.3 настоящего пункта.

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

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

1.22 Постоянный анализ рисков достигается путем наблюдения за функционированием Платежной Системы, выявления риск-событий, определенных в профилях рисков Платежной Системы, либо идентификации новых риск-событий, требующих оценки и пересмотра профилей рисков Платежной Системы.

1.23 Мониторинг рисков осуществляется путем наблюдения за соответствием уровня остаточного риска после применения способов управления рисками уровню допустимого риска, указанного в пункте 1.19 настоящего Порядка, при возникновении новых риск-событий и расчета и анализа динамики изменения значений КИР.

1.24 Оценка эффективности мероприятий по восстановлению оказания УПИ в Платежной Системе осуществляется посредством сопоставления фактического времени восстановления оказания УПИ, в случае приостановления оказания, и фактического времени восстановления УПИ в соответствии с требованиями к оказанию услуги соответствующим значениям, определенным в пункте 1.26 настоящего Порядка.

1.25 Мероприятия по управлению значимыми рисками и непрерывностью функционирования Платежной Системы признаются неэффективными при двукратном и более превышении времени восстановления оказания УПИ, установленного Оператором в пункте 1.26.1 настоящего Порядка. В иных случаях управление значимыми рисками и непрерывностью функционирования Платежной Системы признаются эффективными.

1.26 Оператор устанавливает время устранения инцидента, восстановления УПИ, в том числе в соответствии с требованиям к оказанию услуг.
1.26.1 Время восстановления услуг при приостановлении их оказания – 6 часов с момента нарушения УПИ;
1.26.2 Время восстановления в соответствии с требованиями к оказанию услуг – 72 часа с момента нарушения требований к оказанию услуг.

2 Управление непрерывностью функционирования Платежной Системы

2.1 Управление непрерывностью осуществляется посредством выявления риск-событий, их регистрации в базе риск-событий риска, оценки влияния на БФПС каждого инцидента, применение мер, в том числе Плана действий, направленных на обеспечение непрерывности деятельности и (или) восстановление деятельности Оператора в случае возникновения нестандартных и чрезвычайных ситуаций (далее «**План ОНиВД**»), в отношении инцидентов.

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

2.2.1 время и дата возникновения инцидента (в случае невозможности установить время возникновения инцидента указывается время его выявления);

2.2.2 краткое описание инцидента (характеристика произошедшего риск-события и его последствия);

2.2.3 наименование одного или нескольких бизнес-процессов, в ходе которых произошел инцидент;

2.2.4 наименование одного или нескольких бизнес-процессов, на которые инцидент оказал влияние;

2.2.5 наличие (отсутствие) факта приостановления (прекращения) оказания УПИ в результате инцидента;

2.2.6 влияние инцидента на БФПС;

2.2.7 степень влияния инцидента на функционирование Платежной Системы в зависимости от количества операторов УПИ, и (или) количества и значимости Участников, на которых оказал непосредственное влияние инцидент, и (или) количества и суммы неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников;

2.2.8 время и дата восстановления оказания УПИ в случае приостановления их оказания;

2.2.9 мероприятия по устранению неблагоприятных последствий инцидента с указанием планируемой и фактической продолжительности проведения данных мероприятий;

2.2.10 дата восстановления оказания УПИ, соответствующего требованиям к оказанию услуг;

2.2.11 неблагоприятные последствия инцидента по субъектам Платежной Системы, в том числе:

2.2.11.1 сумма денежных средств, уплаченных Оператором и (или) взысканных с Оператора;

2.2.11.2 сумма денежных средств, уплаченных Оператором УПИ и (или) взысканных с Оператора УПИ;

2.2.11.3 количество и сумма неисполненных, и (или) несвоевременно исполненных, и (или) ошибочно исполненных распоряжений Участников, на исполнение которых оказал влияние инцидент;

2.2.11.4 продолжительность приостановления оказания УПИ.

2.3 Оператор собирает сведения об инцидентах с субъектов Платежной Системы, указанные в перечне в пункте 2.2 настоящего Порядка, при этом сведения, указанные в пунктах 2.2.6 и 2.2.7 настоящего Порядка предоставляются только Операторами УПИ.

2.4 Оператор проводит оценку влияния на БФПС каждого произошедшего в Платежной Системе инцидента в срок не позднее рабочего дня, следующего за днем возникновения (выявления) инцидента, а также в срок не позднее окончания рабочего дня, следующего за днем устранения последствий инцидента (восстановления оказания УПИ, соответствующих требованиям к оказанию услуг), и оценку влияния на БФПС всех инцидентов, произошедших в Платежной Системе за календарный месяц, в течение пяти рабочих дней после дня окончания календарного месяца, в котором возникли инциденты.

2.5 Оператор определяет КИР, указанные в Приложении №2 к настоящему Порядку, и устанавливает и пересматривает с использованием результатов оценки рисков в Платежной Системе их пороговые уровни.

2.6 Оператор и Операторы УПИ рассчитывают фактические значения КИР, анализируемые за предыдущий календарный месяц, в отношении оказываемых ими услуг не позднее пятого рабочего дня, следующего за окончанием анализируемого календарного месяца.

2.7 Операторы УПИ направляют Оператору рассчитанные значения КИР по форме Приложения №6 к настоящему Порядку в разрезе оказываемых ими услуг по заранее согласованным каналам связи не позднее пятого рабочего дня, следующего за окончанием анализируемого календарного месяца.

2.8 По результатам ежемесячной оценки Оператор составляет отчет о сведениях по инцидентам, возникшим при оказании УПИ, и значениям КИР, анализирует динамику изменения значений КИР,

рассчитываемых за месяц, и составляет график изменения значений КИР. Указанный отчет является частью набора отчетов оценки СУР в Платежной Системе.

2.9 В случае если вследствие произошедшего в Платежной Системе инцидента нарушен регламент выполнения процедур, но при этом не нарушен пороговый уровень каждого из показателей П1, П2, данный инцидент признается непосредственно не влияющим на БФПС.

2.10 В случае если вследствие инцидента в Платежной Системе реализовано хотя бы одно из перечисленных ниже условий, данный инцидент признается непосредственно влияющим на БФПС:
2.10.1 нарушен регламент выполнения процедур при одновременном нарушении порогового уровня показателя П2;
2.10.2 нарушен пороговый уровень показателя П1;
2.10.3 превышена продолжительность установленного Оператором времени, в течение которого должно быть восстановлено оказание УПИ, соответствующее требованиям к оказанию услуг.

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

2.12 В случае если вследствие произошедших в Платежной Системе в течение календарного месяца инцидентов одновременно нарушены пороговые уровни всех показателей П3, П4, П5, рассчитанных по данным инцидентам, данные инциденты признаются влияющими на БФПС.
2.13 В случае выявления дополнительных обстоятельств инцидентов, произошедших в течение месяца, по которому была завершена оценка, Оператор проводит повторную оценку влияния на БФПС с учетом вновь выявленных обстоятельств за данный месяц в течение пяти рабочих дней после завершения месяца, в котором выявлены новые обстоятельства инцидента.

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

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

2.16 Оператор устанавливает порядок изменения операционных и технологических средств и процедур:

2.16.1 Оператор вправе изменять операционные и технологические средства и процедуры по своему усмотрению в следующих случаях:
2.16.1.1 в случае изменения порядка оказания услуг или вида услуг;
2.16.1.2 в случаях, предусмотренных законодательством Российской Федерации;
2.16.1.3 по требованию Банка России;
2.16.1.4 в рамках СУР;
2.16.1.5 в результате проведения оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией.
2.16.2 Изменение операционных и технологических средств и процедур осуществляется в следующем порядке:
2.16.2.1 С инициативой об изменении операционных и технологических средств и процедур может выступить Оператор или Оператор УПИ. Кроме того, Участники имеют право направлять Оператору предложения по изменению операционных и технологических средств и процедур;
2.16.2.2 Для целей принятия решения о необходимости изменения операционных и технологических средств и процедур Оператор проводит консультации с Операторами УПИ. При этом, с учетом характера и масштаба планируемых изменений операционных и технологических средств и процедур Оператор и Операторы УПИ могут принять решение о формировании совместной комиссии по изменению операционных и технологических средств и процедур, которая функционирует в период внедрения соответствующих изменений. Персональный состав, срок и объем полномочий такой комиссии определяется совместным протоколом Оператора и Оператора УПИ;
2.16.2.3 Оператор и Операторы УПИ могут принять решение о необходимости формирования комиссии, указанной в п. 2.16.2.2. выше, в качестве постоянно действующего органа, который на регулярной основе рассматривает вопросы, связанные с достаточностью операционных и технологических средств и процедур. В случае принятия решения о формировании такого постоянно действующего органа, Оператор и Оператору УПИ обязаны определить его персональный состав, полномочия и порядок функционирования;
2.16.2.4 Оператор имеет право самостоятельно принимать решение о необходимости изменения операционных и технологических средств и процедур в случае, если такие изменения необходимы в силу требований законодательства Российской Федерации или в силу требований Банка России;
2.16.2.5 Оператор (или комиссия, сформированная Оператором и Операторами УПИ) имеет право привлекать третьих лиц в качестве экспертов для целей проведения оценки необходимости внесения изменений в операционные и технологические средства и процедуры.
2.16.3 В случае если изменение операционных и технологических средств и процедур Оператором требует внесения изменений в Правила, Оператор вносит соответствующие изменения в порядке, предусмотренном Правилами.
2.16.4 В случае если изменение операционных и технологических средств и процедур Оператором приводит к изменению условий Оферты, Оператор направит Участнику новую Оферту об изменении в порядке, предусмотренном Правилами.
2.16.5 В случае если изменение операционных и технологических средств и процедур Оператором не требует внесения изменений в Правила и не приводит к изменению условий Оферты, Оператор направляет Участникам уведомление об изменении операционных и технологических средств и процедур с описанием таких изменений не позднее, чем за тридцать календарных дней до даты вступления в силу соответствующих изменений.
2.16.6 Участник вправе самостоятельно вносить изменения в операционные и технологические средства и процедуры по взаимодействию с Платежной Системой на стороне Участника в случае, если внесение таких изменений не противоречит Правилам Платежной Системы, условиям Оферты, законодательству Российской Федерации и не приводит к изменению порядка оказания услуг, предусмотренного Правилами, а также к объему и характеру услуг, оказываемых Участникам.

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

2.17.1 при наличии в Платежной Системе одного Оператора УПИ (Операционного, и/или Платежного клирингового, и/или Расчетного центра) Оператор обеспечивает привлечение другого Оператора УПИ и переход Участников на обслуживание к вновь привлеченному Оператору УПИ в случаях:

2.17.1.1 превышения Оператором УПИ времени восстановления оказания УПИ при приостановлении их оказания более двух раз в течение трех месяцев подряд;

2.17.1.2 нарушения Правил, выразившегося в отказе Оператора УПИ в одностороннем порядке от оказания услуг Участнику (Участникам), не связанного с приостановлением (прекращением) участия в Платежной Системе в случаях, предусмотренных Правилами;

2.17.2 при возникновении условий, указанных в пункте 2.17.1 настоящего Порядка Оператор предпринимает следующие шаги:

2.17.2.1 служба управления рисками Оператора подготавливает отчет о нарушениях работы Оператора УПИ в течение рабочего 1 дня и направляет его Генеральному директору;

2.17.2.2 служба управления рисками Оператора проводит сбор внутренней рабочий группы Оператора в течение 1 рабочего дня;

2.17.2.3 Генеральный директор по итогам консультаций рабочей группой принимает решение по привлечению другого Оператора УПИ в течение 5 рабочих дней; Генеральный директор может корректировать дальнейшие шаги по переходу к вновь привлеченному Оператору УПИ и сроки их выполнения;

2.17.2.4 в случае наличия договоров с резервными Операторами УПИ:

2.17.2.4.1 Оператор направляет уведомление резервному Оператору УПИ в течение 1 дня с момента решения о переходе на резервного Оператора УПИ;

2.17.2.4.2 Оператор проводит переговоры для уточнения текущих условий и планов, если это необходимо, в течение 1 недели с момента решения о переходе на резервного Оператора УПИ;

2.17.2.4.3 Рабочая группа разрабатывает детальный план перехода, определяет ключевые задачи и ответственных лиц, а также разрабатывает резервный план на случай возникновения непредвиденных ситуаций в течение 2 недель с момента решения о переходе на резервного Оператора УПИ;

2.17.2.4.4 Рабочая группа совместно резервным Оператором УПИ проводит техническую интеграцию и тестирование систем в течение 1,5 месяца с момента решения о переходе на резервного Оператора УПИ;

2.17.2.4.5 Оператор совместно с резервным Оператором УПИ проводят обучение сотрудников в течение 1,5 месяца с момента решения о переходе на резервного Оператора УПИ;

2.17.2.4.6 Оператор осуществляет постепенный перевод Участников на обслуживание к резервному Оператору УПИ в течение 3 недель с момента завершения технической интеграции;

2.17.2.4.7 рабочая группа осуществляет мониторинг и оценку работы Оператора УПИ в течение 3 месяцев с момента начала перевода Участников на обслуживание к резервному Оператору УПИ;

2.17.2.4.8 рабочая группа подготавливает отчеты по результатам мониторинга деятельности Оператора УПИ и направляет их Генеральному директору; при необходимости вносятся коррективы в соглашение об уровне обслуживания (SLA) резервного Оператора УПИ.

2.17.2.5 в случае отсутствия договоров с резервными Операторами УПИ:

2.17.2.5.1 рабочая группа проводит исследование рынка, запрос коммерческих предложений в течение 1 недели с момента принятия решения о привлечении другого Оператора УПИ;

2.17.2.5.2 Генеральный директор совместно с рабочей группой оценивает коммерческие предложения, принимая во внимание критерии надежности, деловой репутации, технологической совместимости и пр. в течение 2-3 недель с момента принятия решения о привлечении другого Оператора УПИ;

2.17.2.5.3 Оператор проводит переговоры и осуществляет выбор нового Оператора УПИ в течение 4 недель с момента принятия решения о привлечении другого Оператора УПИ;

2.17.2.5.4 Оператор заключает договор и соглашение об уровне обслуживания (SLA) с новым Оператором УПИ, в т.ч. проводит юридическую экспертизу в течение 2 недель с момента выбора нового Оператора УПИ;

2.17.2.5.5 Рабочая группа разрабатывает детальный план перехода, определяет ключевые задачи и ответственных лиц, а также разрабатывает резервный план на случай возникновения непредвиденных ситуаций в течение 2 недель с момента заключения договора с новым Оператором УПИ;

2.17.2.5.6 Рабочая группа совместно новым Оператором УПИ проводит техническую интеграцию и тестирование систем в течение 1 месяца с момента заключения договора с новым Оператором УПИ;
2.17.2.5.7 Оператор совместно с новым Оператором УПИ проводят обучение сотрудников в течение 1 месяца с момента заключения договора с новым Оператором УПИ;
2.17.2.5.8 Оператор осуществляет постепенный перевод Участников на обслуживание к привлеченному Оператору УПИ в течение 3 недель с момента завершения технической интеграции;
2.17.2.5.9 рабочая группа осуществляет мониторинг и оценку работы нового Оператора УПИ в течение 3 месяцев с момента начала перевода Участников на обслуживание к новому Оператору УПИ;
2.17.2.5.10 рабочая группа подготавливает отчеты по результатам мониторинга деятельности нового Оператора УПИ и направляет их Генеральному директору; при необходимости вносятся коррективы в соглашение об уровне обслуживания (SLA) нового Оператора УПИ.
2.18 Оператор определяет основные требования к обеспечению БФПС субъектами Платежной Системы:
2.18.1 субъекты Платежной Системы совместно осуществляют деятельность по обеспечению БФПС в Платежной Системе, при этом функции контроля находится у Оператора;
2.18.2 для обеспечения БФПС Оператор обязан обеспечивать:
2.18.2.1 собственную финансовую устойчивость, поддержание ликвидности;
2.18.2.2 сбор, систематизацию и хранение информации о переводах денежных средств в соответствии с требованиями законодательства и Правилами;
2.18.2.3 принятие мер, направленных на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих оказание УПИ, включая услуги платежного клиринга и расчетные услуги;
2.18.2.4 принятие профилактических мер (выполнение регламентов) для технологических средств, устройств, информационных систем, обеспечивающих оказание УПИ, включая услуги платежного клиринга и расчетные услуги;
2.18.2.5 принятие мер по отказоустойчивости операционных и технологических средств, устройств и информационных систем при возникновении инцидентов, повлекших приостановление оказания операционных услуг, и (или) услуг платежного клиринга, и (или) расчетных услуг;
2.18.2.6 проведение анализа причин нарушения функционирования операционных и технологических средств, устройств и информационных систем, выработку мер по их устранению;
2.18.2.7 соблюдение регламента, определенного для операционных услуг, услуг платежного клиринга и расчетных услуг Платежной Системы;
2.18.2.8 общий контроль за функционированием Платежной Системы и обеспечением БФПС;
2.18.2.9 проведение оценки влияния инцидентов на БФПС в соответствии с методикой, установленной в настоящем Порядке;
2.18.2.10 проведение мероприятий по восстановлению оказания УПИ в случае возникновения инцидентов, повлекших приостановление оказания операционных услуг, и (или) услуг платежного клиринга, и (или) расчетных услуг, в соответствии с установленным регламентом (Приложение №1 к настоящему Порядку);
2.18.2.11 проведение оценки СУР в Платежной Системе;
2.18.2.12 проведение мероприятий по недопущению нарушения БФПС, в том числе связанных с риском потери ликвидности Платежной Системы, кредитный риском Платежной Системы, правовым риском Платежной Системы, операционным риском Платежной Системы, общим коммерческим риском Платежной Системы;
2.18.2.13 проведение прочих мероприятий по своему усмотрению, направленных на обеспечение БФПС;
2.18.3 для обеспечения БФПС Операторы УПИ обязаны обеспечивать:
2.18.3.1 собственную финансовую устойчивость, поддержание ликвидности;
2.18.3.2 принятие мер, направленных на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих оказание УПИ;
2.18.3.3 принятие профилактических мер (выполнение регламентов) для технологических средств, устройств, информационных систем, обеспечивающих оказание УПИ;

2.18.3.4 принятие мер по отказоустойчивости операционных и технологических средств, устройств и информационных систем при возникновении инцидентов в работе Оператора УПИ;
2.18.3.5 проведение анализа причин нарушения функционирования операционных и технологических средств, устройств и информационных систем, выработку мер по их устранению;
2.18.3.6 соблюдение регламента, определенного для Операторов УПИ;
2.18.3.7 своевременное информирование Оператора об инцидентах, касающихся функционирования Платежной Системы;
2.18.3.8 проведение мероприятий по восстановлению оказания УПИ в случае возникновения инцидентов, повлекших приостановление оказания УПИ привлеченным Оператором УПИ, в соответствии с установленным регламентом;
2.18.3.9 проведение оценки влияния инцидентов на БФПС в соответствии с методикой, установленной в настоящем Порядке;
2.18.3.10 сверку результатов расчета значений КИР с Оператором;
2.18.3.11 проведение мероприятий по недопущению нарушения БФПС, в том числе связанными с риском потери ликвидности, кредитным риском, правовым риском, операционным риском, общим коммерческим риском;
2.18.3.12 по запросу Оператора предоставлять информацию о мерах, принимаемых по обеспечению бесперебойности оказания УПИ, в случае увеличения рисков нарушения БФПС;
2.18.3.13 проведение прочих мероприятий, направленных на обеспечение БФПС, по своему усмотрению, не противоречащих требованиям законодательства Российской Федерации, нормативным документам Банка России и настоящему Порядку;
2.18.4 для обеспечения БФПС Участники обязаны обеспечивать:
2.18.4.1 собственную финансовую устойчивость, поддержание ликвидности;
2.18.4.2 принятие мер, направленных на недопущение нарушений функционирования операционных и технологических средств, устройств, информационных систем, обеспечивающих оказание услуг;
2.18.4.3 принятие профилактических мер (выполнение регламентов) для технологических средств, устройств, информационных систем, обеспечивающих оказание услуг;
2.18.4.4 принятие мер по отказоустойчивости операционных и технологических средств, устройств и информационных систем при возникновении инцидентов в работе Участника;
2.18.4.5 проведение анализа причин нарушения функционирования операционных и технологических средств, устройств и информационных систем, выработку мер по их устранению на стороне Участника;
2.18.4.6 соблюдение регламента, определенного для Участника;
2.18.4.7 своевременное информирование Оператора об инцидентах, касающихся функционирования Платежной Системы;
2.18.4.8 проведение мероприятий по восстановлению оказания услуг Участником в случае возникновения инцидентов;
2.18.4.9 проведение прочих мероприятий, направленных на обеспечение БФПС, по своему усмотрению, не противоречащих требованиям законодательства Российской Федерации, нормативным документам Банка России и настоящему Порядку.
2.19 Оператор определяет регламенты для субъектов Платежной Системы в следующих документах:
2.19.1 В Правилах;
2.19.2 В договорах с субъектами Платежной Системы и/или в офертах;
2.19.3 В инструкциях, предоставленных Оператором субъектам Платежной Системы.
2.20 Оператор разрабатывает и включает в План ОНиВД мероприятия, направленные на управление непрерывностью функционирования Платежной Системы в случае возникновения инцидентов, связанных с приостановлением оказания УПИ или нарушением установленных уровней оказания УПИ;
2.21 Оператор анализирует эффективность мероприятий по восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг, и использует полученные результаты при управлении рисками в Платежной Системе;
2.22 Оператор разрабатывает, проверяет (тестирует) и пересматривает План ОНиВД с периодичностью не реже одного раза в два года;

2.23 Оператор обеспечивает оказание УПИ при возникновении инцидентов, а также организует в течение установленных периодов времени восстановление оказания услуг Операторами УПИ в случае приостановления их оказания и восстановление оказания УПИ, соответствующего требованиям к оказанию услуг, в случае нарушения указанных требований.

2.24 Оператор устанавливает порядок перехода на резервный комплекс программных и (или) технических средств при совмещении в Платежной Системе функций Оператора и Операционного, и (или) Расчетного центров, и (или) Центрального Платежного Клирингового Контрагента (ЦПКК):

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

2.24.2 При выходе из строя основного комплекса программных и (или) технических средств осуществляется:

2.24.2.1 Перевод пользователей на резервный комплекс программных и (или) технических средств:

2.24.2.1.1 с использованием горячего резервного копирования при наличии;

2.24.2.1.2 при невозможности перехода на резервный комплекс с горячим резервным копированием реализуется схема перевода пользователей на работу с комплексом с использованием холодного резервного копирования;

2.24.2.2 Определение вышедшей из строя компоненты и восстановление основного комплекса программных и (или) технических средств;

2.24.2.3 Перевод пользователей на основной комплекс программных и (или) технических средств.

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

2.25.1 Формирование рабочей группы из числа работников Оператора и привлеченных экспертов для проведения мероприятий по анализу оценке события, восстановлению процессов, нарушенных вследствие неработоспособности систем и сервисов поставщиков услуг;

2.25.2 Анализ причин и последствий события, проведение оценки влияния на события на УПИ и БФПС;

2.25.3 Информирование Участников Платежной Системы и Банка России в случае приостановления оказания УПИ;

2.25.4 Переключение на услуги резервного поставщика услуг при наличии такого поставщика услуг для затронутого процесса, либо поиск нового поставщика, оказывающего аналогичные услуги, если применимо;

2.25.5 Проведение восстановительных мероприятий совместно с поставщиком услуг по восстановлению оказания УПИ, если событие, связанное с неработоспособностью систем и сервисов поставщика услуг, оказало влияние на оказание УПИ;

2.25.6 Разработка рекомендаций для поставщика услуг, допустившего неработоспособность систем и сервисов, нарушение предоставления которых способно привести к приостановлению оказания УПИ;

2.25.7 Проведение анализа истории событий, связанных с неработоспособностью систем и сервисов поставщика услуг, нарушение предоставления которых привело к приостановлению оказания УПИ;

2.25.8 Проведение мероприятий по недопущению возникновения подобных событий в будущем.

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

2.26.1 Участник Платежной Системы обязан иметь банковский счет не менее чем в двух Расчетных центрах для целей восстановления оказания УПИ в случае возникновении риск-событий, повлекших сбой в оказании услуг;

2.26.2 в случае принятия Участником Платежной Системы решения об осуществлении расчетов через альтернативный Расчетный Центр, Участник уведомит о таком решении Оператора в письменном виде

не менее чем за два рабочих дня до планируемой даты начала расчетов через альтернативный Расчетный Центр;

2.26.3 в случае приостановления оказания УПИ Расчетным Центром, Расчетный Центр, приостановивший оказание УПИ, обязан проинформировать Оператора о приостановлении оказания УПИ в течение 1 часа с момента приостановления оказания УПИ. Начиная с 2 часов после приостановления оказания УПИ альтернативный Расчетный Центр обеспечивает осуществление услуг единственного Расчетного Центра до восстановления оказания УПИ в соответствии с требованиями к оказанию услуг;

2.26.4 в течение 2 часов после устранения причин приостановления оказания УПИ в соответствии с требованиями оказания услуг Расчетный Центр, который устранил такие причины, обязан уведомить Оператора о восстановлении оказания УПИ в соответствии с требованиями оказания услуг. Начиная со следующего рабочего дня услуги Расчетного центра переходят в штатный режим, действующий до приостановления оказания УПИ в одном из Расчетных центров;

координацию возврата в штатный режим, а также уведомление Участников о соответствующих изменениях в оказании услуг осуществляет Оператор.

2.27 Оператор устанавливает порядок обеспечения взаимозаменяемости Операторов УПИ, выполняющих функцию Операционного центра и Центрального Платежного Клирингового Контрагента (ЦПКК) при наличии в Платежной Системе Операционных центров и Центральных Платежных Клиринговых Контрагентов, соответственно:

2.27.1 между Оператором и Операторами УПИ устанавливаются единые стандарты для протоколов обмена информацией и форматов данных;

2.27.2 обеспечивается совместимость программных и аппаратных решений;

2.27.3 Оператором совместно с Операторами УПИ организуются системы резервного копирования и дублирования данных;

2.27.4 Организация Оператором взаимодействия между Операторами УПИ, включая заключение соглашений между Операторами УПИ, определяющих условия их взаимодействия, обмен данными, совместное использование ресурсов и пр.;

2.27.5 Оператором совместно с Операторами УПИ обеспечивается защита данных на всех уровнях, включая шифрование и противодействие киберугрозам при использовании каналов взаимодействия.

2.27.6 Процесс переключения между Операционного центра и Центрального Платежного Клирингового Контрагента (ЦПКК) включает в себя:

2.27.6.1 Уведомление Участников и заинтересованных лиц при необходимости в течение 1 рабочего дня;

2.27.6.2 Проверка готовности резервного Оператора УПИ к приему нагрузки от основного Оператора УПИ в течение 2 часов;

2.27.6.3 Перенаправление операций на резервного Оператора УПИ в течение 4 часов;

2.27.6.4 Контроль проведения восстановительных мероприятий, проводимых основным Оператором УПИ;

2.27.6.5 Мониторинг операций, перенаправленных на резервного Оператора УПИ в течение 3 рабочих дней;

2.27.6.6 После проведения восстановительных мероприятий основным Оператором УПИ подготовка к обратному переключению на основного Оператора УПИ в течение 2 часов;

2.27.6.7 Перенаправление операций на основного Оператора УПИ в течение 4 часов;

2.27.6.8 Проведение анализа процесса переключения.

2.27.6.9 Контроль проведения мероприятий по недопущению возникновения подобных событий в будущем.

3 Организация взаимодействия субъектов Платежной Системы по обеспечению БФПС

3.1 В соответствии с Правилами Оператор может запросить субъектов Платежной Системы о предоставлении информации, касающейся деятельности в качестве субъекта Платежной Системы для целей оценки рисков и влияния на БФПС в Платежной Системе в форме адресных запросов и/или интервью и/или анкетирования;

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

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

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

- предусмотренных законодательством Российской Федерации;
- если информация является публичной;
- если получено предварительное письменное согласие владельца информации;
- в случаях, предусмотренных Правилами.

3.5 В случае выявления Оператором нарушений в части обеспечения БФПС субъектом Платежной Системы Оператор информирует субъекта Платежной Системы о таком факте в день выявления Оператором нарушения посредством направления соответствующего сообщения по электронной почте в адрес такого субъекта Платежной Системы;

3.6 Оператор осуществляет проверку устранения нарушений субъектом Платежной Системы в части обеспечения БФПС доступными способами, в том числе, в случае наличия такой возможности, проверку доступности оказываемой субъектом Платежной Системы услуги;

3.7 Субъекты Платежной Системы вправе запрашивать разъяснения процедур, отраженных в настоящем Порядке;

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

3.9 Порядок информирования Банка России и субъектов Платежной Системы о приостановлении и восстановлении оказания УПИ.

3.9.1 Оператор информирует:

Банк России в порядке, предусмотренном законодательством Российской Федерации и документами Банка России;

Субъекты Платежной Системы о случаях и причинах приостановления (прекращения) оказания УПИ в день такого приостановления (прекращения) путем направления соответствующего уведомления по электронной почте на адрес Субъекта Платежной Системы, указанный в Заявлении на участие в Платежной Системе, и / или путем размещения на официальном сайте в информационно-телекоммуникационной сети Интернет (www.omnypay.ru);

3.9.2 По факту восстановления обеспечения УПИ в Платежной Системе Оператор уведомляет об этом субъектов Платежной Системы и Банк России в день восстановления путем направления соответствующего уведомления по электронной почте на адрес Субъекта Платежной Системы,

указанный в Заявлении на участие в Платежной Системе, и / или путем размещения на официальном сайте в информационно-телекоммуникационной сети Интернет (www.omnypay.ru).

3.10 Порядок взаимодействия в спорных, нестандартных и чрезвычайных ситуациях.

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

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

3.10.3 К обстоятельствам непреодолимой силы относятся риск-события, на которые субъекты Платежной Системы не могут оказывать влияние и за возникновение которых не несут ответственности, например, землетрясение, наводнение, стихийные бедствия, пожар, а также забастовка, террористические акты, правительственные постановления или распоряжения государственных органов, военные действия любого характера или срывы в работе системы расчетов между банками и небанковскими кредитными организациями на территории Российской Федерации или за ее пределами, которые препятствуют исполнению субъектами Платежной Системы своих обязательств;

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

3.10.5 Уведомление о наступлении обстоятельств непреодолимой силы направляется субъектами Платежной Системы следующим образом:

Участник и Оператор УПИ, находящийся под воздействием обстоятельств непреодолимой силы, направляет уведомление Оператору;

Оператор, находящийся под воздействием обстоятельств непреодолимой силы, направляет уведомление всем Участникам и Операторам УПИ.

3.11 В случае возникновения споров между субъектами Платежной Системы такие споры разрешаются в порядке, предусмотренном Правилами.

4 Контроль за соблюдением субъектами Платежной Системы БФПС

4.1 Оператор осуществляет контроль порядка обеспечения БФПС субъектами Платежной Системы следующими способами:

4.1.1 сбор, документирование и анализ сведений об инцидентах, получаемых от субъектов Платежной Системы;

4.1.2 использование сведений об инцидентах в оценках СУР и обеспечения БФПС;

4.1.3 оценка динамики изменения количества инцидентов посредством расчета соответствующих КИР;

4.1.4 детальный анализ существенных инцидентов, причин их возникновения, сроки устранения;

4.1.5 анкетирование и/или интервью и/или адресные запросы, проведение самооценки субъектов Платежной Системы с целью получения сведений, необходимых для использования в мероприятиях по контролю порядка обеспечения БФПС субъектами Платежной Системы;
4.1.6 направление запросов Операторам УПИ на предоставление внутренних документов по БФПС;
4.1.7 работа с информацией по жалобам клиентов;
4.1.8 оценка СУР;
4.1.9 контроль финансового состояния субъектов Платежной Системы посредством кредитного анализа финансовой отчетности;
4.1.10 установление лимитов обязательств Участников;
4.1.11 тестирование доступности оказания УПИ, в том числе доступности услуги у Участников.
4.2 Оператор доводит до сведения субъектов Платежной Системы информацию о выявленных недостатках в области обеспечения БФПС и рекомендации по их устранению по доступным каналам связи по выбору Оператора (по эл. почте, путем размещения на эл. ресурсе в сети Интернет и пр.).

5 Организационная структура для обеспечения бесперебойности функционирования Платежной Системы

5.1 Организационная структура для обеспечения бесперебойности функционирования Платежной Системы включает следующие уровни:
5.2 Исключительный уровень управления рисками в Платежной Системе, а также обеспечения бесперебойности функционирования Платежной Системы – Совет Директоров Оператора (в случае его формирования);
5.3 На первом уровне управления рисками в Платежной Системе, а также обеспечения бесперебойности функционирования Платежной Системы действуют:
5.3.1 сотрудники структурных подразделений Оператора, осуществляющие бизнес-процессы Платежной Системы, ответственные за управление рисками и обеспечение бесперебойности функционирования в Платежной Системе в рамках своих полномочий, определенных должностными инструкциями, внутренними документами и приказами (далее «СПоБП»);
5.3.2 руководители структурных подразделений Оператора, осуществляющих бизнес-процессы Платежной Системы, ответственных за управление рисками и обеспечение бесперебойности функционирования в Платежной Системе в отношении оказываемых Операторами УПИ услуг в рамках своих полномочий, определенных должностными инструкциями, внутренними документами и приказами (далее «Руководители СПоБП»);
5.3.3 назначенные привлеченными Операторам УПИ сотрудники (далее «СОУПИ»), ответственные за управление рисками и обеспечение бесперебойности функционирования в Платежной Системе в отношении оказываемых Операторами УПИ услуг.
5.4 На втором уровне управления рисками в Платежной Системе, а также обеспечения бесперебойности функционирования Платежной Системы действуют:
5.4.1 Генеральный директор Оператора;
5.4.2 структурные подразделения Оператора, уполномоченные на выполнение отдельных функций по управлению рисками (далее «СПУР»). Перечень таких структурных подразделений определен в Стратегии управления рисками и капиталом Оператора;
5.5 На третьем уровне управления рисками в Платежной Системе, а также обеспечения бесперебойности функционирования Платежной Системы действует:
5.5.1 Служба внутреннего аудита Оператора (далее «СВА»).

5.6 Обеспечение БФПС первого уровня организационной структуры Платежной Системы выполняется СПоБП, Руководителями СПоБП и сотрудниками привлеченных Операторов УПИ при выполнении ими бизнес-процессов Платежной Системы.

5.7 Обеспечение БФПС второго уровня организационной структуры Платежной Системы выполняется Генеральным директором в части контрольных и организационных мероприятий, а также

при принятии решений о БФПС в рамках своих полномочий, и СПУР в части методологических функций по управлению рисками, присущих бизнес-процессам, и при координировании процессов управления рисками между Оператором и привлеченными Операторами УПИ.

5.8 Обеспечение БФПС на третьем уровне организационной структуры Платежной Системы выполняется СВА в части оценки СУР Платежной Системы.

5.9 Руководители СПоБП выполняют следующие функции:
5.9.1 осуществляют контроль за обеспечением БФПС своими структурными подразделениями;
5.9.2 принимают решение о реагировании на инциденты в зависимости от степени воздействия на УПИ в соответствии с Приложением №5 к настоящему Порядка, в том числе о принятии ответных мер и активации сценариев Плана ОНиВД (за исключением решений, которые относятся к компетенции Генерального директора Оператора);
5.9.3 обеспечивают формирование и поддержание в актуальном состоянии описания бизнес-процессов;
5.9.4 обеспечивают идентификацию рисков, присущих бизнес-процессам;
5.9.5 участвуют в проведении оценки значимых рисков;
5.9.6 обеспечивают осведомленность своих сотрудников СПоБП о значимых рисках и порядке управления ими в соответствии с разработанными внутренними документами;
5.9.7 разрабатывают внутренние инструкции, методики, положения для СПоБП на основе методик и процедур, определенных сотрудниками второго уровня;
5.9.8 предоставляют информацию для составления профилей рисков и согласовывают сведения в профиле рисков, составленный на основании проведенной оценки;
5.9.9 предоставляют предложения о реагировании на значимые риски;
5.9.10 обеспечивают подготовку, тестирование и пересмотр Плана ОНиВД в рамках своей зоны ответственности за бизнес-процессы и системы;
5.9.11 направляют предложения по дополнительным КИР (если требуется их введение) и обеспечивают выполнение установленных КИР;
5.9.12 обеспечивают предоставление информации для анализа рисков Платежной Системы;
5.9.13 обеспечивают выявление и регистрацию риск-событий;
5.9.14 обеспечивают полноту и корректность сведений о зарегистрированных риск-событиях;
5.9.15 обеспечивают своевременное доведение информации о риск-событиях и БФПС до сотрудников организационной структуры Платежной Системы второго уровня;
5.9.16 предоставляют информацию по риск-событиям для оценки влияния на БФПС;
5.9.17 предоставляют информацию для отчетов о БФПС.

5.10 СОУПИ выполняют следующие функции в отношении оказываемых соответствующими Операторами УПИ услуг:
5.10.1 осуществляют контроль за обеспечением БФПС;
5.10.2 обеспечивают идентификацию рисков;
5.10.3 предоставляют Оператору информацию для анализа рисков Платежной Системы;
5.10.4 участвуют в проведении оценки значимых рисков;
5.10.5 предоставляют информацию Оператору для составления профилей рисков и согласовывают сведения в профиле рисков, составленный на основании проведенной оценки;
5.10.6 предоставляют Оператору предложения о реагировании на значимые риски;
5.10.7 направляют предложения по дополнительным КИР (если требуется их введение) и обеспечивают выполнение установленных КИР;
5.10.8 обеспечивают полноту и корректность сведений о зарегистрированных риск-событиях;
5.10.9 обеспечивают своевременное доведение информации о риск-событиях и БФПС до сотрудников организационной структуры Платежной Системы второго уровня;
5.10.10 предоставляют рассчитанные значения КИР в соответствии с пунктом 2.7 настоящего Порядка.

5.10.11
5.10.12 Генеральный директор Оператора выполняет следующие функции:
5.10.13 утверждает профили рисков Платежной Системы;
5.10.14 рассматривает отчеты о БФПС;
5.10.15 принимает решения о реагировании на инциденты в зависимости от степени воздействия на УПИ в соответствии с Приложением №5 к настоящему Порядку;
5.10.16 согласовывает предложения по Способам управления рисками;
5.10.17 согласовывает предложения по дополнительным КИР (если требуется их введение);
5.10.18 обеспечивает принятие решений о применении Способов управления рисками с целью обеспечение непрерывности функционирования Платежной Системы в условиях риск-события при приостановлении оказания УПИ на срок, превышающий допустимый уровень, в том числе об активации сценариев Плана ОНиВД;
5.10.19 принимает решение по спорным вопросам, по вопросам с отсутствующей согласованной позицией сотрудников первого уровня организационной структуры Платежной Системы;
5.10.20 организует процедуру информирования заинтересованных лиц о влиянии на БФПС с учетом установленных порядков;
5.10.21 утверждает отдельные процедуры по управлению рисками в Платежной Системе в рамках своих полномочий и в соответствии с настоящим Порядком;
5.10.22 распределяет полномочия, обязанности и ответственность между структурными подразделениями в области управления рисками и обеспечения БФПС;
5.10.23 утверждает внутренние документы Оператора в области управления рисками.
5.10.24
5.10.25 Служба управления рисками Оператора выполняет следующие функции:
5.10.26 разрабатывает и поддерживает в актуальном состоянии Порядок обеспечения БФПС и прочие внутренние документы, регламентирующие управление рисками и обеспечение БФПС;
5.10.27 разрабатывает методологию управления рисками и бесперебойности функционирования Платежной Системы;
5.10.28 организует выполнение процедур по управлению рисками в соответствии с методологическими указаниями;
5.10.29 рассматривает отчеты и/или информацию о риск-событиях, предоставленную Руководителями СПоБП и субъектами Платежной Системы;
5.10.30 осуществляет анализ рисков на основе предоставляемой информации, характеризующей риск-событие;
5.10.31 осуществляет мониторинг рисков в соответствии с пунктом 1.23 настоящего Порядка, контролирует своевременное применение Способов управления рисками;
5.10.32 совместно с Руководителями СПоБП и СОУПИ осуществляет идентификацию рисков Платежной Системы, присущих бизнес-процессам;
5.10.33 осуществляет оценку значимых рисков Платежной Системы;
5.10.34 составляет, поддерживает в актуальном состоянии профили рисков Платежной Системы;
5.10.35 осуществляет оценку влияния риск-событий Платежной Системы на УПИ;
5.10.36 информирует Генерального директора и Совет Директоров Оператора об инцидентах при приостановлении оказания УПИ на срок, превышающий допустимый уровень;
5.10.37 организует процедуры контроля обеспечения БФПС субъектами Платежной Системы;
5.10.38 организует процедуру информирования субъектов Платежной Системы о выявленных недостатках в БФПС и направления рекомендаций по устранению недостатков;
5.10.39 проводит стресс-тестирование значимых рисков Платежной Системы;
5.10.40 составляет отчеты о БФПС;
5.10.41 предоставляет СПУР рекомендации для осуществления методологических функций;
5.10.42 формирует и направляет отчетность об обеспечении БФПС регулирующим органам;
5.10.43 проводит анализ систематических проблем и совместно с Руководителями СПоБП и СОУПИ разрабатывает меры по повышению эффективности управления рисками.
5.10.44

5.10.45 СПУР выполняют следующие функции:

5.10.46 разрабатывают методологию управления рисками и бесперебойности функционирования Платежной Системы по отдельным направлениями деятельности в рамках своей компетенции;

5.10.47 контролируют выполнение процедур согласно разработанным методологическим указаниям.

5.10.48

5.10.49 Совет Директоров Оператора выполняет следующие функции:

5.10.50 рассматривает и утверждает отчеты о БФПС;

5.10.51 утверждает План ОНиВД;

5.10.52 дает рекомендации по внесению изменений в Порядок обеспечения БФПС;

5.10.53 дает рекомендации по внесению изменений в профиль рисков Платежной Системы;

5.10.54 рассматривает материалы по результатам оценки СУР в Платежной Системе.

5.10.55

5.10.56 СВА Оператора обеспечивает следующие функции:

5.10.57 проводит проверку эффективности методологии оценки рисков и процедур управления рисками, установленных внутренними документами Платежной Системы и полноты применения указанных документов;

5.10.58 Информирует Совет Директоров Оператора о выявленных несоответствиях.

Приложение №1
к Порядку обеспечения БФПС

Регламент выполнения процедур в Платежной Системе

Наименование УПИ	Наименование процедуры	Время выполнения процедуры УПИ
Операционная услуга	Передача распоряжения по отправлению/выдаче переводов денежных средств в Платежную Систему (включая контрольные процедуры по приему/выдаче распоряжения).	Не более 10 минут
Услуга платежного клиринга	Расчет платежных клиринговых позиций по состоянию на операционный день.	• Длительность процедуры: не более 2-х часов в течение рабочего дня, следующего за днем приема распоряжения по отправлению/выдаче переводов денежных средств в Платежную Систему; • Время окончания процедуры: не позднее 1 часа до завершения операционного дня Расчетного центра.
	Предоставление отчетной информации Участникам по всем распоряжениям Участника, принятым в Платежную Систему.	• Длительность процедуры: не более 2-х часов в течение рабочего дня, следующего за днем принятия распоряжения по отправлению/выдаче переводов денежных средств в Платежную Систему; • Время окончания процедуры: не позднее окончания дня, следующего за днем принятия распоряжения по отправлению/выдаче переводов денежных средств в Платежную Систему.
	Подготовка и передача в Расчетный центр реестра платежных клиринговых позиций.	• Длительность процедуры: не более 1-го часа; • Время окончания процедуры: не позднее первого рабочего дня, следующего за днем расчета платежных клиринговых позиций и не позднее 30 минут до завершения операционного дня Расчетного центра.
Расчетная услуга	Исполнение платежных клиринговых позиций согласно полученному реестру при условии достаточности остатка денежных средств на корреспондентских счетах Участников для проведения соответствующих платежных клиринговых позиций.	• Длительность процедуры: не более 2-х часов; • Время окончания процедуры: не позднее текущего операционного дня, в котором был получен реестр платежных клиринговых позиций.

Приложение №2
к Порядку обеспечения БФПС

Мониторинг уровней значимых рисков

1. Для оценки риска БФПС в соответствии с требованиями выделяет следующие КИР:

1.1. показатель продолжительности восстановления оказания УПИ (далее «показатель П1»), характеризующий период времени восстановления оказания услуг Операторами УПИ в случае приостановления оказания УПИ, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных нормативными документами Банка России;

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

1.3. показатель соблюдения регламента (далее «показатель П3»), характеризующий соблюдение Операторами УПИ времени начала, времени окончания, продолжительности и последовательности процедур, выполняемых Операторами УПИ при оказании операционных услуг, услуг платежного клиринга и расчетных услуг, предусмотренных частями 3 и 4 статьи 17, частью 4 статьи 19 и частями 1 и 8 статьи 25 Федерального закона №161-ФЗ (далее «регламент выполнения процедур»);

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

1.5. показатель изменения частоты инцидентов (далее «показатель П5»), характеризующий темп прироста частоты инцидентов.

2. Порядок расчета КИР и их пороговые значения:

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

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

2.1.2. показатель П1 должен рассчитываться в часах/минутах/секундах;

2.1.3. пороговый уровень показателя П1 <= 6 часов;

2.2. показатель П2 должен рассчитываться по каждому из Операторов УПИ при возникновении каждого из инцидентов, повлекших приостановление оказания УПИ, как период времени между двумя последовательно произошедшими у Оператора УПИ инцидентами, в результате которых приостанавливалось оказание УПИ, с момента восстановления оказания УПИ, приостановленных в результате первого инцидента, и до

момента возникновения события, приведшего к приостановлению оказания УПИ в результате следующего инцидента;

2.2.1. В платежных системах, в которых Оператор УПИ оказывает более одного вида УПИ одновременно, показатель П2 должен рассчитываться одновременно по всем видам УПИ, оказываемым данным Оператором УПИ;

2.2.2. показатель П2 должен рассчитываться в часах/минутах/секундах;

2.2.3. пороговый уровень показатель П2 >= 6 часов;

2.3. показатель П3 должен рассчитываться по каждому Оператору УПИ;

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

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

где:

$N_{оц}$ - количество распоряжений Участников (их клиентов), по которым в течение календарного месяца были оказаны операционные услуги без нарушения регламента выполнения процедур;

$N_{оц}^{общ}$ - общее количество распоряжений Участников (их клиентов), по которым были оказаны операционные услуги в течение календарного месяца;

2.3.1.1. Пороговый уровень показателя $П3_{оц}$ >= 98.00%;

2.3.2. для Платежного Клирингового Центра показатель П3 должен рассчитываться как отношение количества распоряжений Участников (их клиентов), по которым в течение календарного месяца были оказаны услуги платежного клиринга без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников (их клиентов), по которым были оказаны УПИ в течение календарного месяца, рассчитываемое по следующей формуле:

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

где:

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

$N_{пкц}^{общ}$ - общее количество распоряжений Участников (их клиентов), по которым были оказаны услуги платежного клиринга в течение календарного месяца;

2.3.2.1. Пороговый уровень показателя $П3_{пкц}$ >= 98.00%;

2.3.3. для Расчетного Центра показатель П3 должен рассчитываться как отношение количества распоряжений Участников и (или) Платежного Клирингового Центра, по которым в течение календарного месяца были оказаны расчетные услуги без нарушения регламента выполнения процедур, к общему количеству распоряжений Участников и (или) Платежного Клирингового Центра, по которым были оказаны расчетные услуги в течение календарного месяца, рассчитываемое по следующей формуле:

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

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;

2.3.4. показатель П3 должен рассчитываться ежемесячно в процентах с точностью до двух знаков после запятой (с округлением по математическому методу);

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

2.3.6. в платежных системах, в которых Оператор УПИ оказывает более одного вида УПИ одновременно, показатель П3 должен рассчитываться по данному Оператору УПИ в отношении всех видов оказываемых им услуг;

2.3.7. Пороговый уровень показателя $П3_{рц}$ >= 99.00%;

2.4. показатель П4 должен рассчитываться 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;

2.4.1. показатель П4 должен рассчитываться ежемесячно в процентах с точностью до двух знаков после запятой (с округлением по математическому методу);

2.4.2. для платежных систем с несколькими Операционными Центрами показатель П4 должен рассчитываться для каждого Операционного Центра Платежной Системы;

2.4.3. значение показателя П4 по Платежной Системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем Операционным Центрам Платежной Системы;

2.4.4. пороговый уровень показателя П4 >= 96.00%;

2.5. показатель П5 должен рассчитываться по Платежной Системе в целом и для каждого Оператора УПИ в отдельности как темп прироста среднедневного количества инцидентов за оцениваемый календарный месяц по отношению к среднедневному количеству инцидентов за предыдущие двенадцать календарных месяцев, включая оцениваемый календарный месяц, рассчитываемый по следующей формуле:

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

,

где:

$КИ_i$ - 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 двенадцать предыдущих календарных месяцев, включая оцениваемый месяц;

2.5.1. показатель П5 должен рассчитываться ежемесячно в процентах с точностью до одного знака после запятой (с округлением по математическому методу). В случае если за предыдущие двенадцать календарных месяцев, включая оцениваемый месяц, инцидентов не было, значение показателя признается равным нулю. В случае если за предыдущие двенадцать календарных месяцев, включая оцениваемый месяц, в шести месяцах не было инцидентов, при этом за оцениваемый месяц количество инцидентов не превышает 10, значение показателя признается равным нулю;

2.5.2. в платежных системах, в которых Оператор УПИ оказывает более одного вида УПИ одновременно, показатель П5 должен рассчитываться по данному Оператору УПИ в отношении всех видов оказываемых им услуг;

2.5.3. пороговый уровень показателя П5 <= 300%.

3. Оператор может разрабатывать и применять дополнительные КИР.

3.1. Дополнительные КИР разрабатываются с учетом следующего:

3.1.1. требований законодательства Российской Федерации и нормативных актов Банка России, регламентирующих Платежную Систему;

3.1.2. сведений о риск-событиях;

3.1.3. результатах мониторинга уровня риска;

3.1.4. прочих требований, свидетельствующих о целесообразности разработки дополнительных КИР.

Приложение №3
к Порядку обеспечения БФПС

Критерии существенности (значимости) риск-событий

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

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

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

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

3. Матрица, характеризующая уровень влияния на деятельность Платежной Системы (воздействие риска на деятельность).

3.1. Критерии существенности по операционным услугам:

3.1.1. Для целей оценки риск-события по критериям существенности для расчета количества операций переводов денежных средств, ожидаемых за календарный день, в котором произошло риск-событие, определяется среднее количество операций переводов денежных средств за предыдущие календарные дни, в которых не было риск-событий, соответствующие по объему оцениваемому календарному дню. В случае отсутствия достоверных, и (или) актуальных, и (или) полных, и (или) релевантных данных для расчета количества операций переводов денежных средств, ожидаемых за календарный день, расчет осуществляется с использованием экспертной оценки.

Критерий	**Риск-событие или инцидент**	**Нарушение УПИ**	**Уровни оказания УПИ**
Сбой, не влияющий на приостановление (прекращение) Операционных услуг	Риск-событие (0)	Нет	Штатный режим
Сбой, влияющий на 0.01% - 15% количества операций денежных переводов	Риск-событие (0)	Нет	Штатный режим
Сбой, влияющий на 15.01% - 20% количества операций денежных переводов	Инцидент низкий (1)	Нет	Штатный режим
Сбой, влияющий на 20.01% - 40% количества операций денежных переводов	Инцидент умеренный (2)	Нет	Штатный режим

Сбой, влияющий на 40.01% - 90% количества операций денежных переводов	Инцидент средний (3)	Нет	Ограниченный режим
Сбой, влияющий на >90.00% количества операций денежных переводов	Инцидент высокий (4)	Да	Приостановление

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

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

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

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

3.3. Критерии существенности по риск-событиям информационной безопасности.

Критерий	Риск-событие или инцидент	Нарушение УПИ	Уровни оказания УПИ
Риск-событие, нарушившее информационную безопасность в инфраструктуре Участника (отсутствуют	Риск-событие (0)	Нет	Штатный режим

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

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

3.4. По рискам, находящимся в зеленой или желтой зонах, решение о применении мер реагирования принимается на уровне руководителей подразделений; по рискам, находящимся в оранжевой и красной зонах, решение о применении мер реагирования принимается на уровне Правления.

3.5. Прочие риск-события рассматриваются как не влияющие на УПИ.

3.6. События, следствием которых является приостановление оказания УПИ в связи с проведением технологических и (или) регламентных работ, в случае если Оператор УПИ заранее уведомил об этом Оператора и Участников Платежной Системы в соответствии с правилами и (или) иными документами Оператора и (или) привлеченных Операторов УПИ, не относятся к событиям приостановления оказания УПИ.

4. Качественная оценка риска (уровень риска) определяется умножением значения, определенного по матрице чувствительности к риску (вероятности (частоты) реализации риска), на значение, определенного по матрице влияния на деятельность Платежной Системы (воздействия риска) (Приложение №5 к настоящему Порядку).

Приложение №4
к Порядку обеспечения БФПС

Профиль риска и требования к его заполнению

1. Профили рисков должны составляться по всем значимым рискам в Платежной Системе, в том числе по:
   1.1. Правовому риску Платежной Системы (по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие несоблюдения субъектами Платежной Системы требований законодательства Российской Федерации, Правил, договоров, заключенных между субъектами Платежной Системы, документов Оператора и документов Операторов УПИ либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России, Правилах и договорах, заключенных между субъектами Платежной Системы, а также вследствие нахождения Операторов УПИ и Участников под юрисдикцией различных государств);
   1.2. Операционному риску Платежной Системы (по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие возникновения у субъектов Платежной Системы сбоев, отказов и аварий в работе информационных и технологических систем, недостатков в организации и выполнении технологических и управленческих процессов, ошибок или противоправных действий персонала субъектов Платежной Системы, либо вследствие воздействия событий, причины возникновения которых не связаны с деятельностью субъектов Платежной Системы, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц);
   1.3. Кредитному риску Платежной Системы (по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, Центральным Платежным Клиринговым Контрагентом или Расчетным Центром Платежной Системы вследствие невыполнения Участниками договорных обязательств перед указанными организациями в установленный срок или в будущем);
   1.4. Риску ликвидности Платежной Системы (по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие отсутствия у Платежного Клирингового Центра и (или) у Участников денежных средств, достаточных для своевременного выполнения их обязательств перед другими субъектами Платежной Системы);
   1.5. Общему коммерческому риску Платежной Системы (по риску оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие ухудшения финансового состояния Оператора и (или) Операторов УПИ, не связанного с реализацией кредитного риска Платежной Системы и риска ликвидности Платежной Системы).

2. Перечень причин возникшего риск-события в Платежной Системе:

Причина возникшего (выявленного) инцидента	**Код**
Нарушения Оператором УПИ бизнес-процессов в Платежной Системе, в том числе вследствие ненадлежащей организации бизнес-процессов, нарушения выполнения бизнес-процессов, внутренних регламентов и процедур	01

Нарушения в работе персонала и в организации труда Оператора УПИ, в том числе вследствие превышения сотрудниками своих полномочий, ошибочных противоправных действий и (или) бездействия персонала	02
Нарушения в работе систем, оборудования и технологий Оператора УПИ, не связанных с нарушением безопасности и защиты информации, в том числе по причине невыполнения поставщиками (провайдерами) услуг, предоставляющими или поддерживающими системы и сервисы, необходимые для оказания Оператором УПИ услуг платежной инфраструктуры, своих обязательств, включая неработоспособность систем и сервисов поставщиков (провайдеров) услуг	03
Нарушения в работе систем, оборудования и технологий у Оператора УПИ, связанных с нарушением безопасности и защиты информации, в том числе в результате реализации компьютерных атак	04
Несоблюдение Правил, договоров об оказании операционных услуг и (или) платежных клиринговых услуг, и (или) договоров банковского счета	05
Нарушения в деятельности Оператора УПИ по причине обстоятельств непреодолимой силы, в частности стихийных бедствий, технологических катастроф, недобросовестных действий третьих лиц, применения мер организациями и ведомствами, в том числе центральными (национальными) банками иностранных государств в рамках международных санкций	06
Несоблюдение Правил и (или) договоров, заключенных с Оператором УПИ, об оказании операционных услуг и (или) платежных клиринговых услуг, если заключение таких договоров предусмотрено Правилами	07
Несоблюдение Участником (Участниками) Правил и (или) договоров об оказании операционных услуг, и (или) платежных клиринговых услуг, и (или) договоров банковского счета, неработоспособность систем и сервисов Участника (Участников)	08
Несоблюдение операционным центром Платежной Системы Правил и (или) договоров об оказании операционных услуг, если заключение таких договоров предусмотрено Правилами, неработоспособность систем и сервисов операционного центра	09
Несоблюдение Платежным клиринговым центром Платежной Системы Правил и (или) договоров об оказании платежных клиринговых услуг, если заключение таких договоров предусмотрено Правилами, неработоспособность систем и сервисов Платежного клирингового центра Платежной Системы	10
Несоблюдение Расчетным центром Центральным платежным клиринговым контрагентом Платежной Системы Правил и (или) договоров, заключенных с Операционным центром и (или) Платежным клиринговым центром Платежной Системы, если заключение таких договоров предусмотрено Правилами, договоров банковского счета, заключаемых с Участниками, неработоспособность систем и сервисов Расчетного центра и (или) Центрального платежного клирингового контрагента Платежной Системы	11
Иные причины возникшего (выявленного) инцидента, не предусмотренные кодами 01 - 11	20

3. Основные Способы управления рисками в Платежной Системе по видам рисков:

Виды рисков	**Способы управления рисками в Платежной Системе**

Платежной Системы	
Правовой риск Платежной Системы	• Предварительная проверка Оператором потенциальных Участников и Операторов УПИ на обладание необходимой правоспособностью; • Периодическая, не реже одного раза в год, выборочная проверка Оператором Участников и Операторов УПИ на обладание необходимой правоспособностью путём запросов на предоставление необходимой информации об их деятельности и документов, в том числе внутренних документов и договоров; • Ежедневный мониторинг банковских операций на предмет выявления возможных рисков и несоответствий действующему законодательству; • Анализ нормативно-правовой документации на предмет соответствия требованиях законодательства действующих процессов и новых, разрабатываемых процессов и процедур; • Периодический инструктаж сотрудников, периодическая проверка знаний сотрудников, доведение до сведений сотрудников изменений в законодательстве и внутренних процедур.
Операционный риск Платежной Системы	• Разработка технических требований на создание, внедрение и эксплуатацию аппаратно-программных комплексов с учётом требований к показателям бесперебойности; • Тестирование аппаратно-программных комплексов перед их внедрением; • Регулярный мониторинг системного, прикладного программного обеспечения и доступа к информационным ресурсам; • Обеспечение целостности информационных активов путём применения: средств идентификации и аутентификации, процедур протоколирования и аудита, криптографической защиты информации, резервного копирования и архивирования информационных ресурсов; • Обеспечение резервирования критичных информационных активов; разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев; • Проведение регулярной оценки качества и надёжности функционирования информационных систем, операционных и технологических средств, соответствие их отраслевым нормативным актам; • Сбор, систематизация, обработка, анализ и хранение информации об инцидентах в Платежной Системе; • Анализ потенциальных источников операционного риска при заключении новых договоров, сделок, разработки новых банковских продуктов, технологий, построение схем, моделей, созданий процедур; • Включение в договоры с Расчетным центром условий об обеспечении бесперебойности функционирования процедур, а также штрафных санкции в случае возникновения операционного риска;

	• Проведение регламентных работ по обеспечению БФПС; • Ограничение функций и полномочий на системном уровне; • Обучение персонала; • Введение скриптов, регламентов и инструкций для персонала.
Кредитный риск Платежной Системы	• Установление и изменение предельных лимитов обязательств Участников с учетом уровня риска; • Создание гарантийного фонда Платежной Системы. • Автоматизированный контроль остатка на счетах Участников в Расчетных центрах для осуществления клиринга; • Периодическая оценка финансового состояния субъектов Платежной Системы и изменение лимитов по результатам; • Осуществление Расчетным центром кредитования в форме овердрафта банковских счетов Оператора и/или отдельных Участников путем заключения отдельного соглашения между Расчетным центром и Оператором и/или Участником. • Использование гарантийного фонда Платежной Системы для выполнения обязательств Участников; • Осуществление расчетов в пределах, предоставленных Участниками денежных средств; • Осуществление расчетов в Платежной Системе до конца рабочего дня.
Риск потери ликвидности Платежной Системы	• Эффективное управление кредитным риском Платежной Системы во избежание реализации связанного с ним риска потери ликвидности (в силу специфики деятельности организации риск ликвидности Платежной Системы в большинстве случаев может быть следствием реализации кредитного риска Платежной Системы; • Формирование избытка (запаса) ликвидных средств; • Сглаживание дисбаланса между сроками погашения требований и обязательств; • Составление матрицы фондирования в период кризисных ситуаций; • Прогноз позиции денежных средств; • Расчеты на нетто основе; • Инвестирование свободных денежных средств только в высоколиквидные инструменты; • Создание источников фондирования; • управление очередностью исполнения распоряжений Участников.
Общий коммерческий риск Платежной Системы	• Организация и контроль системы принятия решений и делегирования полномочий; • Организация и соблюдение внутренних управленческих правил и процедур, бизнес-процессов; • Достижение планов по финансовому результату; • Планирование расходов в соответствии с планами по финансовому результату; • Применение мер по изменению стратегии в случае возникновения предпосылок по недостижению стратегических планов; • Планирование инвестиций по поддержанию инфраструктуры

	Платежной Системы с обеспечением высокого уровня отказоустойчивости; • Планирование инвестиций в квалифицированный персонал, обеспечивающий высокий уровень поддержки оказания УПИ; • Сохранение высокого уровня деловой репутации.

4. Перечень бизнес-процессов в Платежной Системе:

Перечень бизнес-процессов Платежной Системы	**Код бизнес-процесса**
Выполнение регуляторных требований	Р1
Клиентская поддержка	Р2
Мониторинг и управление рисками	Р3
Обеспечение доступности инфраструктуры Платежной Системы	Р4
Обеспечение офисной инфраструктуры организации	Р5
Операционные услуги	Р6
Расчетные услуги	Р7
Услуга платежного клиринга	Р8
Расширение каналов доступности услуги	Р9
Реализация бизнес-стратегии	Р10

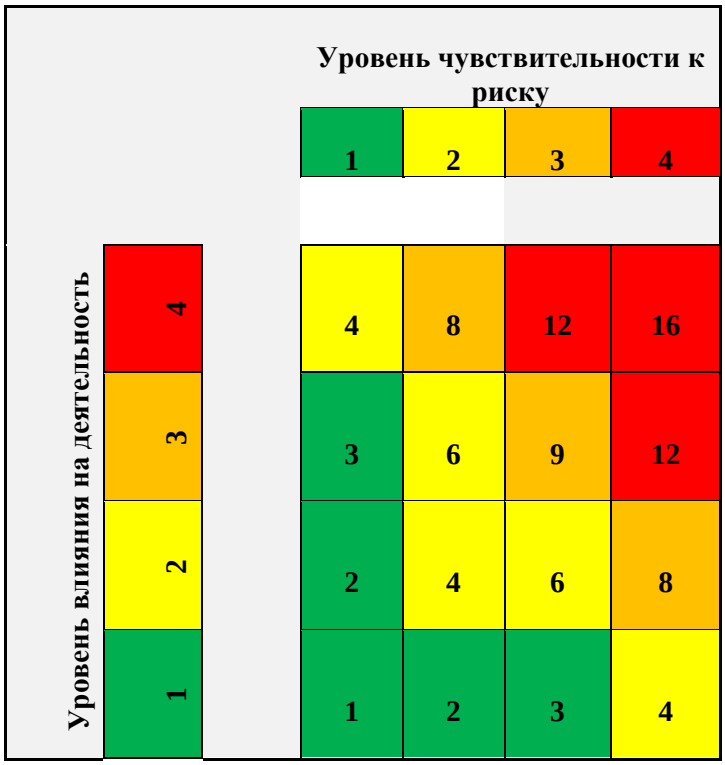
5. Содержание профиля каждого из значимых рисков в Платежной Системе:
   5.1. описание риск-событий, выявленных с применением не менее одного метода из числа предусмотренных Стандартом. Риск-события отражаются в профиле каждого из значимых рисков в Платежной Системе;
   5.2. описание причины возникновения каждого из риск-событий;
   5.3. описание бизнес-процессов, в которых могут произойти риск-события;
   5.4. вероятность наступления риск-событий (определение вероятности наступления риск-событий осуществляется с применением не менее одного метода из числа предусмотренных Стандартом);
   5.5. описание и оценка возможных неблагоприятных последствий каждого риск-события (если риск-событие имеет несколько возможных неблагоприятных последствий, то указываются все неблагоприятные последствия данного риск-события; определение неблагоприятных последствий риск-событий осуществляется с применением методов из числа предусмотренных Стандартом с учетом результатов анализа сведений об инцидентах);
   5.6. описание бизнес-процессов и перечень субъектов Платежной Системы, на которые влияет риск-событие;
   5.7. уровень присущего риска до применения Способов управления рисками в Платежной Системе;
   5.8. уровень допустимого риска;
   5.9. уровень остаточного риска после применения Способов управления рисками в Платежной Системе;
   5.10. перечень Способов управления рисками в Платежной Системе.

6. Профиль риска нарушения БФПС должен составляться в отношении значимых рисков в Платежной Системе
7. Структура профиля рисков для комбинации риск/риск-событие:

Риск	Риск-событие	Метод выявления риск-события	Причины возникновения	Бизнес-процесс, в котором возникло риск-событие	Вероятность наступления	Метод определения вероятности	Способы управления рисками	Описание возможных неблагоприятных последствий	Оценка возможных неблагоприятных последствий	Метод определения последствий	Затронутые Бизнес-процессы	Затронутые субъекты	уровень присущего риска	уровень допустимого риска	уровень остаточного риска	Влияние на БФПС
Кредитный	1.1.						1.1.1.				1.1.1.	1.1.1.1				
												1.1.1.n				
							1.1.2.				1.1.2.	1.1.2.1				
												1.1.2.n				
							1.1.n.				1.1.n.					
	1.n															
Ликвидности	2.1															
	2.n															
Правовой																
Общий коммерческий																
Операционный																

Приложение №5
к Порядку обеспечения БФПС

Качественная характеристика уровня риска



Качественная характеристика уровня риска	Баллы (Уровень влияния на деятельность * Уровень чувствительности к риску)
Хороший уровень (зеленая зона)	1-3
Удовлетворительный уровень (желтая зона)	4-6
Сомнительный уровень (оранжевая зона)	8-9
Неудовлетворительный уровень (красная зона)	12-16

Приложение №6
к Порядку обеспечения БФПС

Наименование организации	
Регистрационный номер	
Отчетный период	

Номер строки	**Наименование показателя**	**Фактическое значение показателя соблюдения регламента выполнения процедур (П3), в процентах**	**Фактическое значение показателя доступности операционного центра платежной системы (П4), в процентах**	**Фактическое значение показателя изменения частоты инцидентов (П5), в процентах**
1	2	3	4	5
1	Операционные услуги			
2	Услуги платежного клиринга		x	
3	Расчетные услуги		x	

Номер строки	**Уникальный номер инцидента**	**Фактическое значение показателя продолжительности восстановления оказания УПИ (П1), в формате ДДД.ЧЧ:ММ**	**Фактическое значение показателя непрерывности оказания УПИ (П2), в формате ДДД.ЧЧ:ММ**	**Соблюдение регламента (Да/Нет)**	**Фактическое значение показателя продолжительности восстановления оказания УПИ в соответствии с требованиями к оказанию услуг, в формате ДДД.ЧЧ:ММ**
1	2	3	4	5	6
Подраздел 1. При оказании операционных услуг					
1.1					
…					
Подраздел 2. При оказании услуг платежного клиринга					
2.1					
…					
Подраздел 3. При оказании расчетных услуг					
3.1					
…					

Приложение № 4
к Правилам Платежной Системы

Тарифы

1. Плата за оказание услуг Операторов Услуг Платежной Инфраструктуры непосредственно с Участников не взимается.

2. В случае внесения изменений к настоящим Правилам, приводящим к взиманию платы за оказание услуг Операторов Услуг Платежной Инфраструктуры, соответствующие тарифы включаются в настоящее приложение.

Приложение № 5
к Правилам Платежной Системы

Плата за перевод
при отправлении переводов денежных средств в российских рублях
для выплаты в долларах США в стране назначения*

Сумма перевода	Плата за перевод
100.00 - 5 000.00	100.00 р.
5 000.01 и более	1.0% от суммы перевода

Плата за перевод
при отправлении переводов денежных средств в российских рублях
для выплаты в российских рублях в стране назначения**

Сумма перевода	Плата за перевод
100.00 - 5 000.00	200 р.
5 000.01 и более	3.0% от суммы перевода

Плата за перевод
при отправлении переводов денежных средств в долларах США
для выплаты в долларах США в стране назначения*

Сумма перевода	Плата за перевод
3.00 - 200.00	3.00 доллара США
200.00 и более	3.0% от суммы перевода

*для стран, где доступна выплата в долларах США (перечень стран и набор сервисов размещается на сайте Оператора)

** для стран, где доступна выплата в рублях (перечень стран и набор сервисов размещается на сайте Оператора)

Приложение № 6
к Правилам Платежной Системы

Общие стандарты защиты информации и передачи данных.
Формат и содержание электронных сообщений.

1. При работе с Платежной Системой и Системой применяются следующие стандарты:

1) ISO 9001:2008,
2) ISO 27001:2013,
3) PCI DSS.

2. Конфиденциальность, целостность и доступность каналов связи обеспечивается с использованием протокола TLS - криптографического протокола, обеспечивающего защищённую передачу данных между узлами в сети Интернет.

TLS используют асимметричную криптографию для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений (RFC 5246, RFC 6176). TLS использует следующие алгоритмы:

• Для обмена ключами и проверки их подлинности применяются комбинации алгоритмов: RSA (асимметричный шифр), Diffie-Hellman (безопасный обмен ключами), DSA (алгоритм цифровой подписи), ECDSA;

• Для симметричного шифрования: RC4, IDEA, Triple DES, SEED, Camellia или AES;

• Для хеш-функций: MD5, SHA, SHA-256/384.

3. Аутентификация осуществляется на основании клиентского и серверного сертификатов формата X.509, который является стандартом ITU-T для инфраструктуры открытых ключей (PKI) и управления привилегиями (PMI) (RFC 1422, RFC 5280).

4. Для обеспечения достоверности и аутентичности информации, используются уникальные имена пользователей (логин) и пароли.

5. Для обеспечения защиты персональных данных при их передаче в рамках Платежной Системы в пределах Российской Федерации по открытым каналам связи должны использоваться программно–аппаратные средства, прошедшие в установленном порядке процедуры оценки соответствия и обладающие действующими сертификатами соответствия, из числа используемых Оператором.

6. При обмене электронными сообщениями такие сообщения могут включать следующую информацию:

- персональные данные получателя/отправителя (включая фамилию и имя, дату рождения, адрес, данные ДУЛ);
- наименования получателя/отправителя юридического лица;
- данные отправляющей/выплачивающей организации (включая наименование, тип, адрес отправления/выплаты, номер терминала и данные оператора);
- трансакционные данные (КНДП, сумма перевода, сумма Платы за перевод, ставка конвертации валют, страна отправления/выплаты, номер счета отправителя/получателя и т.д.);
- маркетинговую информацию (номер участника программы лояльности, сумма

накопленных/использованных баллов, информация о специальных акциях и тарифах);

- иную информацию в зависимости от типа Услуги и страны отправления/выплаты.

Конкретный перечень информации, включаемой в электронное сообщение, определяется в зависимости от типа Услуги, страны отправления/выплаты, способа предоставления Участником доступа к Услугам своим клиентам.

7. При обмене электронными сообщениями используется формат XML, HTML, JSON.

Приложение № 7
к Правилам Платежной Системы

Положение
о порядке сбора данных и информации
об Участниках Платежной Системы
в рамках программы «Знай своего клиента»

1. Общие положения

1.1. Настоящее положение о порядке сбора данных и информации об Участниках Платежной Системы в рамках программы «Знай своего клиента» (далее - «Положение») разработано Оператором, в целях осуществления Оператором деятельности, направленной на ПОД/ФТ/ФРОМУ в соответствии с Главой 10 Правил.

1.2. Все термины, используемые по тексту настоящего Положения с заглавной буквы и не определенные непосредственно в Положении, будут иметь значение, установленное для таких терминов в Правилах.

1.3. Настоящее Положение устанавливает порядок и форму сбора данных и информации о новых и уже существующих Участниках в целях идентификации, анализа и мониторинга Участников и их бенефициарных владельцев.

2. Порядок сбора данных и информации

2.1. В целях первичного сбора и обновления данных и информации об Участниках в рамках программы «Знай своего клиента» Оператор направляет в электронной форме Участникам анкету «Знай своего клиента» (далее - «Анкета») по форме, установленной Оператором.

2.2. Анкета заполняется Участниками в соответствии с инструкциями, содержащимися в Анкете. При этом, Участник обязан указывать в Анкете полную и достоверную информацию, включая данные и информацию о прямых и косвенных владельцах участника, конечных бенефициарах, лицах, оказывающих влияние или осуществляющих контроль в отношении Участника, сотрудниках, ответственных за ПОД/ФТ/ФРОМУ, иную информацию, за исключением случаев, когда предоставление такой информации Участником прямо запрещено в соответствии с требованиями законодательства РФ.

2.3. Данные и информация, указываемые Участником в Анкете, должны быть подтверждены Участником копиями соответствующих документов (копии документов, удостоверяющих личность, копии приказов и иных распорядительных документов, и т.д.).

2.4. Оригинал заполненной Анкеты направляется Участником в адрес Оператора в течение 14 дней с даты получения Участником Анкеты в электронном виде.

2.5. Заполнение Анкеты Участника сотрудниками Оператора не допускается.

2.6. Периодическое обновление Анкеты производится путем повторного заполнения Участником Анкеты в сроки, предусмотренные требованиями законодательства в области ПОД/ФТ/ФРОМУ.

3. Порядок работы Оператора с Анкетой

3.1. Оператор использует данные и информацию, указанные Участником в Анкете, в целях осуществления Оператором деятельности, в соответствии с Главой 10 Правил.

3.2. Персональные данные, содержащиеся в Анкетах, должны обрабатываться Оператором исключительно с согласия субъектов персональных данных. Согласие субъектов предоставляется непосредственно в Анкете субъектами персональных данных. В случае, если Анкета не содержит согласие субъекта персональных данных, указанных в Анкете, Анкета должно содержать подтверждение Участника о том, что персональные данные такого субъекта передаются Оператору с согласия субъекта, полученного Участником. Отказ субъекта персональных данных от предоставления согласия на обработку персональных данных не освобождает Участника от обязательств по заполнению Анкеты.

3.3. Уклонение Участника от заполнения Анкеты, непредставление каких-либо данных и информации, запрашиваемых в Анкете, предоставление недостоверных и(или) неполных сведений Участником в Анкете, непредставление копий подтверждающих документов будут являться нарушением Правил.

Приложение № 8
к Правилам Платежной Системы

Порядок
определения вознаграждения Участника

1. Общие положения

1.1. Настоящий Порядок определения вознаграждения Участника за оказание Услуг в рамках Платежной Системы разработан в целях отражения в Правилах Платежной Системы порядка (в том числе критериев, влияющих на размер вознаграждения Участника) определения размера вознаграждения Участника за оказание Услуг в рамках Платежной Системы.

1.2. Все термины, используемые по тексту настоящего Порядка с заглавной буквы и не определенные непосредственно в настоящем Порядке, будут иметь значение, установленное для таких терминов в Правилах.

2. Вознаграждение Участника

2.1. Вознаграждение Участника представляет собой процент от суммы перевода денежных средств, отправляемого или выплачиваемого Участником. Ставка вознаграждения Участника устанавливается в Оферты об участии в Платежной Системе.

2.2. Вознаграждение, причитающаяся Участнику за оказание Услуг клиентам Участника, устанавливается с учетом положений настоящего Порядка для всех Участников, присоединяющихся к Правилам Платежной Системы.

3. Порядок и критерии определения вознаграждения Участника

3.1. Базовое вознаграждение Участника за оказание Услуг в рамках Платежной Системы составляет 0,16% от суммы перевода денежных средств, отправляемого или выплачиваемого Участником (далее «Базовое вознаграждение»).

3.2. Вознаграждение Участника свыше Базового вознаграждения может быть установлено в зависимости от следующих критериев:

- подключение Участником Отделений в Москве, Санкт-Петербурге и Отделений в местах с низким присутствием Платежной Системы (с учетом общего количества Отделений, количества Отделений в каждом из городов, географии Отделений в каждом городе, наличия Отделений в местах большого скопления потенциальных клиентов и иных факторов);
- обеспечение Участником предоставления доступа своим клиентам к Услугам через Интернет-банк Участника (с учетом общего количества потенциальных пользователей, сроков реализации, потенциального объема переводов и иных факторов);
- обеспечение Участником предоставления доступа своим клиентам к Услугам через мобильное приложение Участника (с учетом общего количества потенциальных пользователей, сроков реализации, потенциального объема переводов и иных факторов);
- осуществление перевода денежных средств по определенным направлениям (входящие и исходящие переводы, переводы по отдельным направлениям и группам стран и т.д с учетом общего количества потенциальных пользователей Услуг среди клиентов Участника, важности соответствующих направлений для Платежной Системы).

3.3. Суммарная ставка вознаграждения, причитающегося Участнику, указывается

Оператором в Оферте и представляет собой сведения, составляющие коммерческую тайну Оператора и Участника. Суммарная ставка вознаграждения, причитающаяся Участнику, может устанавливаться отдельно по направлениям, Услугам и способам предоставления доступа клиентам Участника к Услугам.

3.4. В целях стимулирования и продвижения Услуг, оказываемых Участниками своим клиентам, Оператор вправе предлагать Участникам участвовать в различных программах Оператора, позволяющих Участником получать дополнительное вознаграждение за оказание Услуг при условии достижения показателей, установленных Оператором (далее «Стимулирующие программы»). Такие Стимулирующие программы могут распространяться на определённую территорию, отдельных Участников, отдельные Услуги или отдельные способы предоставления доступа клиентам Участников к Услугам. Для целей включения Участника в Стимулирующую программу, Участнику направляется Оферта об изменении условий участия в Платежной Системе, содержащая условия Стимулирующей программы. В случае согласия Участника с условиями Стимулирующей программы, Участник соглашается с Офертой об изменении условий участия в Платежной Системе путем направления Оператору Акцепта, подписанного Участником.

Приложение № 9
к Правилам Платежной Системы

ФОРМА
ОТЧЕТА ОБ ИНЦИДЕНТАХ

Сведения об инцидентах информационной безопасности, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств в Платежной Системе

Наименование Организации	
Регистрационный номер	
Отчётный период	Место для ввода даты.
Степень выполнения требований к применению организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для выявления инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств (согласно п.8.14 «Правил Платежной Системы»).	☐ **высокая** ☐ **средняя** ☐ **низкая** **Комментарий (для низкой степени):** _____
Информирование, в случае ее наличия, о выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств (согласно п.8.14 «Правил Платежной Системы»).	☐ **не выявлено** ☐ **выявлено** **Количество:** _____
Степень выполнения требований к реагированию на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств (согласно п.8.14 «Правил Платежной Системы)	☐ **высокая** ☐ **средняя** ☐ **низкая** **Комментарий (для низкой степени):** _____
Степень выполнения требований к анализу причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении переводов денежных средств, проведение оценки результатов реагирования на такие инциденты (согласно п.8.14 «Правил Платежной Системы»).	☐ **высокая** ☐ **средняя** ☐ **низкая** **Комментарий (для низкой степени):** _____

Наименование организации
ФИО должностного лица

Приложение № 10
к Правилам Платежной Системы

ФОРМА ПЕРЕЧНЯ ПЛАТЕЖНЫХ СИСТЕМ, С КОТОРЫМИ ОСУЩЕСТВЛЯЕТСЯ ВЗАИМОДЕЙСТВИЕ

Наименование платежной системы	Информация об операторе платежной системы (наименование, адрес, адрес сайта в сети интернет)	Дата начала взаимодействия