УТВЕРЖДЕНО

Протоколом внеочередного общего собрания

Участников ООО «РСМП»

№ 31 от «24» июля 2024г.

Правила
Платежной системы «МОМЕНТОМ»

Версия 12.0

Дата вступления в силу с «26» августа 2024 г.

2024 г.

Запись об операторе платежной системы
внесена в реестр операторов платежных систем
16 февраля 2018 года за регистрационным номером 0047

Введение

I. Оператором Платежной системы «МОМЕНТОМ» (далее по тексту – Платежная система) является Общество с ограниченной ответственностью «РСМП» (ИНН 7716861927; ОГРН 1177746612801) (далее по тексту – Оператор).

II. Настоящие Правила Платежной системы «МОМЕНТОМ» (далее – Правила) разработаны на основании требований Федерального закона «О национальной платежной системе» от 27.06.2011 № 161-ФЗ и принятыми в соответствии с ним нормативными актами Банка России.

III. Настоящие Правила определяют порядок, условия и особенности взаимодействия Оператора, Операторов услуг платежной инфраструктуры и Участников Платежной системы, а также порядок и условия оказания Участниками Услуг по Переводу денежных средств Клиентов на территории Российской Федерации, и в случае оказания Услуг по трансграничному переводу денежных средств Клиентов.

IV. Настоящие Правила являются договором присоединения, который заключается в соответствии со статьей 428 Гражданского кодекса Российской Федерации. Участники присоединяются к Правилам путем принятия их в целом.

V. Настоящие Правила и тарифы (являющиеся частью Правил), публикуются в открытом доступе на Сайте Платежной системы. Толкование Правил осуществляется в рамках законодательства Российской Федерации.

VI. Расчеты в Платежной системе осуществляются в российских рублях, долларах США, ЕВРО и (или) национальных валютах (при необходимости).

VII. Для заключения договора участия в Платежной системе, потенциальный участник Платежной системы направляет Оператору заявление об участии в Платежной системе по форме Приложения № 1.

Оглавление

1. Термины, определения и сокращения

Банковский счет – банковский счет Клиента, открытый у Участника или в любом ином банке, в том числе в иностранном банке.

Банк-Отправитель – Участник, осуществляющий по распоряжению Отправителя Перевод в пользу Получателя за счет денежных средств, находящихся на Банковском счете Отправителя.

Банк-Получатель – Участник, осуществляющий исполнение распоряжения Отправителя о Переводе посредством зачисления денежных средств на Банковский счет Получателя.

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

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

Бизнес-процесс(ы) – один или несколько процессов, в рамках которых обеспечивается оказание УПИ.

Бесперебойность функционирования платежной системы (БФПС) – обеспечение Оператором ПС бесперебойности функционирования ПС, которая достигается при условии оказания Участникам Платежной системы УПИ согласно требованиям Федерального закона от 27 июня 2011 года № 161-ФЗ и принятых в соответствии с ним нормативных актов Банка России, а также положениям Правил Платежной системы, договоров об оказании УПИ, документов Оператора ПС и привлеченных им Операторов УПИ (далее при совместном упоминании - требования к оказанию услуг) и (или) восстановления оказания УПИ, соответствующего требованиям к оказанию услуг, и восстановления оказания УПИ в случае приостановления их оказания в течение периодов времени, установленных Оператором ПС в настоящих Правилах.

Валюта зачисления распоряжения на Перевод денежных средств – валюта зачисленных денежных средств Получателю, и валюта, в которой возникают обязательства Оператора перед Участником, обслуживающим Получателя.

Валюта Перевода денежных средств – валюта, в которой сохраняется Перевод денежных средств в рамках ПС; может отличаться от Валюты приема распоряжения на Перевод денежных средств и от Валюты зачисления распоряжения на Перевод денежных средств.

Валюта приема распоряжения на Перевод денежных средств – валюта принятых денежных средств от Отправителя и валюта, в которой возникают обязательства Участника, обслуживающего Отправителя.

Гарантийный фонд ПС (Гарантийный фонд) – инструмент для обеспечения исполнения обязательств Участников в ПС «МОМЕНТОМ» по трансграничным переводам.

ДБО – дистанционное банковское обслуживание **–** услуги по Переводу, оказываемые через системы интернет-банкинга и т.п.

Закон о НПС – Федеральный закон «О национальной платежной системе» от 27.06.2011 N 161-ФЗ.

Защищаемая информация – информация, относимая к информации ограниченного доступа и подлежащая защите, в соответствии с законодательством Российской Федерации, в том числе Законе о НПС, а также на основании Правил и внутренних документов Оператора. Виды защищаемой информации определены в п. 10.2.1 Правил.

ИБ – информационная безопасность.

Интернет (Сеть Интернет) – информационно-телекоммуникационная сеть, которая не является доверенной сетью Оператора, эксплуатация и пользование которой реализуется неопределенным числом субъектов, что создает риски ИБ.

Инцидент – событие, которое привело к нарушению оказания УПИ и (или) соответствующих требований к оказанию услуг, в том числе требований к обеспечению защиты информации, описанных в разделе 10 Правил.

ИТ – информационные технологии.

ИТ-подразделение – структурное подразделение Оператора, которое, согласно соответствующему положению, несет ответственность за эксплуатацию и (или) администрирование ИТ-инфраструктуры Оператора и поддержание работоспособности автоматизированных систем и приложений Оператора.

Клиент – Отправитель, Получатель.

Косвенный Участник – Участник, которому открыл банковский (корреспондентский) счет Прямой Участник, являющийся оператором по переводу денежных средств, в целях осуществления расчета с другими Участниками.

Мобильное приложение – программный комплекс на мобильных устройствах различного типа для обеспечения доступа Клиентов к Услугам по Переводу денежных средств в рамках Платежной системы.

Окончательность Перевода – характеристика Перевода денежных средств, обозначающая предоставление денежных средств Получателю в определенный момент времени.

ОНиВД – обеспечение непрерывности и восстановления деятельности, план действий, направленный на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения нестандартных и чрезвычайных ситуаций, включая инциденты.

Оператор Платежной системы (Оператор) – ООО «РСМП» (ИНН 7716861927; ОГРН 1177746612801), определяющее Правила Платежной системы, а также выполняющее иные обязанности, предусмотренные Законом о НПС и Правилами Платежной системы.

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

Операционный центр – ООО «РСМП» (ИНН 7716861927; ОГРН 1177746612801)**,** обеспечивающее в рамках Платежной системы для Участников и Клиентов доступ к услугам по Переводу денежных средств, а также обмен электронными сообщениями, содержащими распоряжения Участников.

Отправитель – юридическое лицо/индивидуальный предприниматель/физическое лицо - клиент Участника, дающий распоряжение Участнику на осуществление в рамках Платежный системы Перевода денежных средств.

Партнер Платежной системы (Партнер). В качестве Партнера могут быть**:**

- российское юридическое лицо (в том числе оператор по переводу денежных средств), оказывающее услуги по взаимодействию с ПС «МОМЕНТОМ» на основании заключенного отдельного соглашения/договора с Оператором.

– иностранное юридическое лицо, имеющее (при необходимости) лицензию на осуществление Переводов денежных средств в соответствии с требованиями иностранного законодательства своего местонахождения. Партнер осуществляет взаимодействие с ПС «МОМЕНТОМ» на основании заключенного отдельного соглашения/договора с Оператором.

Перевод денежных средств (Перевод) – действия Оператора по переводу денежных средств в рамках применяемых форм безналичных расчетов по предоставлению Получателю денежных средств Отправителя. Перевод денежных средств осуществляется посредством списания денежных средств с Банковского счета Отправителя, для зачисления на Банковский счет Получателя.

Платежная система «МОМЕНТОМ» (ПС «МОМЕНТОМ», Платежная система, ПС) – совокупность организаций, объединенных единым информационным пространством и взаимодействующих в соответствии с настоящими Правилами в целях осуществления Переводов денежных средств, включая Оператора, Операторов услуг платежной инфраструктуры и Участников.

Платежный клиринговый центр – ООО «РСМП» (ИНН 7716861927; ОГРН 1177746612801), обеспечивающее в рамках Платежной системы прием к исполнению распоряжений Участников об осуществлении Перевода денежных средств и выполнение иных действий, предусмотренных Законом о НПС.

Получатель – юридическое лицо/индивидуальный предприниматель/физическое лицо - Клиент Участника, в пользу которого направлены денежные средства Отправителя.

Прямой Участник – Участник, который открыл банковский (корреспондентский) счет (Счет Участника) в Расчетном центре в целях осуществления расчетов с другими Участниками.

Расчетный центр – организация, созданная в соответствии с законодательством Российской Федерации и обеспечивающая в рамках Платежной системы исполнение распоряжений Участников посредством списания и зачисления денежных средств по Счетам, а также направление подтверждений, касающихся исполнения распоряжений Участников.

Реестр нетто-позиций – документ или совокупность документов, содержащих информацию, необходимую Расчетному центру/Участникам для осуществления расчетов в рамках Платежной системы за определенный период времени, составляемый и предоставляемый Платежным клиринговым центром в электронной форме.

Риск-событие - событие, реализация которого может привести к возникновению Инцидента.

Сайт Платежной системы – официальный сайт в информационно-телекоммуникационной сети «Интернет», размещенный по адресу www.momentom.su.

СКЗИ – средства криптографической защиты информации, классифицируемые таковыми согласно требованиям ФСБ России, в том числе Приказа ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

Согласованный канал связи (Личный кабинет) – программный комплекс (в том числе ДБО), доступ к которому осуществляется с использованием сети «Интернет» через Сайт Платежной системы. Личный кабинет обеспечивает информационное и технологическое взаимодействие между Субъектами Платежной системы. В контексте взаимодействия между Оператором и Банком России под Согласованным каналом (каналами) связи подразумевается техническая инфраструктура (автоматизированной системы) Банка России или резервные способы информационного взаимодействия с Банком России, согласно размещаемой на официальном сайте Банка России в сети «Интернет» информации.

Стандарт – национальный стандарт Российской Федерации ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска», утвержденный и введенный в действие приказом Федерального агентства по техническому регулированию и метрологии от 17 декабря 2019 г. № 1405-ст «Об утверждении национального стандарта Российской Федерации».

Субъекты Платежной системы – Оператор, Операторы услуг платежной инфраструктуры и Участники.

Счет Участника (Счет Прямого Участника / Счет Косвенного Участника) – банковский (корреспондентский) счет, предназначенный для проведения расчетов по операциям, совершенным в Платежной системе. Открывается Расчетным центром Прямому Участнику на условиях договора, заключаемого между Прямым Участником и Расчетным центром. Счет Косвенного Участника открывается Прямым Участником Косвенному Участнику, на условиях договора банковского счета, заключаемого между Косвенными Участником и Прямым Участником.

Тарифы – документ, являющийся неотъемлемой частью настоящих Правил (Приложение № 2), и устанавливающий размер стоимости оказания Услуг по Переводу денежных средств в ПС «МОМЕНТОМ», размер вознаграждения Субъектов ПС и величину комиссии, взимаемой с Отправителя.

Трансграничный перевод - перевод денежных средств, при осуществлении которого Отправитель либо Получатель средств находится за пределами Российской Федерации, и (или) перевод денежных средств, при осуществлении которого Отправителя или Получателя средств обслуживает иностранный центральный (национальный) банк или иностранный банк.

Требования к оказанию услуг – требования, применяемые к Оператору Платежной системы при обеспечении бесперебойности функционирования Платежной системы, которая достигается при условии оказания Участникам Платежной системы услуг платежной инфраструктуры согласно требованиям Федерального закона от 27 июня 2011 года № 161-ФЗ «О национальной платежной системе» и принятых в соответствии с ним нормативных актов Банка России, а также положениям настоящих Правил Платежной системы «МОМЕНТОМ», договоров об оказании УПИ, документов Оператора Платежной системы и привлеченных им Операторов УПИ.

УПИ – услуги платежной инфраструктуры, включая услуги операционного, клирингового и расчетного центров.

Управление непрерывностью функционирования Платежной системы – выявление оказания УПИ, не соответствующего требованиям к оказанию услуг, обеспечению функционирования Платежной системы «МОМЕНТОМ» в случае нарушения оказания УПИ, соответствующего требованиям к оказанию услуг, и восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг, включая восстановление оказания УПИ в случае приостановления их оказания в течение периодов времени, установленных Оператором Платежной системы в настоящих Правилах Платежной системы «МОМЕНТОМ».

Управление рисками в Платежной системе - организация системы управления рисками в Платежной системе, обеспечивающая бесперебойность функционирования Платежной системы.

Услуги Платежной системы (Услуги) – осуществление исполнения Перевода денежных средств (в том числе трансграничного Перевода денежных средств) в ПС «МОМЕНТОМ» путем списания денежных средств со Счета Участника/Партнера, обслуживающего Отправителя, и зачисления денежных средств на Счет Участника/Партнера, обслуживающего Получателя, или осуществляющего Перевод в его пользу.

Участник (Прямой/Косвенный Участник):

- **Участники-резиденты РФ** - операторы по переводу денежных средств, органы Федерального казначейства, страховые организации (осуществляющие обязательное страхование гражданской ответственности в соответствии с законодательством Российской Федерации), организации федеральной почтовой связи, присоединившиеся к настоящим Правилам;

- **Участники-нерезиденты** - международные финансовые организации, иностранные центральные (национальные) банки, иностранные банки, иностранные поставщики платежных услуг, присоединившиеся к настоящим Правилам, в том числе с учетом требований соответствующего иностранного законодательства.

Федеральный закон № 115-ФЗ – Федеральный закон от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»

2. Общие положения о Правилах

2.1. Порядок осуществления контроля за соблюдением Правил

2.1.1. Контроль за соблюдением настоящих Правил Операционным центром, Платежным клиринговым центром, Участниками и Расчетным центром осуществляет Оператор на постоянной основе путем мониторинга их деятельности в процессе оказания услуг в рамках Платежной системы, анализа жалоб и обращений Клиентов.

2.1.2. В целях контроля за соблюдением настоящих Правил Оператор с использованием Согласованных каналов связи осуществляет следующие мероприятия:

- получает от Участников и Расчетного центра информацию об их деятельности, в том числе по оказанию Услуг по Переводу денежных средств в рамках Платежной системы (при необходимости);
- направляет запросы в целях получения от них (Расчетного центра и Участников) необходимых документов и пояснений, касающихся спорных ситуаций;
- организует внутренний информационный документооборот между Операционным центром, Платежным клиринговым центром и Оператором;
- организует прием и обработку обращений по вопросам функционирования Платежной системы;
- проверяет и анализирует полученную информацию, в том числе для обеспечения в Платежной системе защиты информации при осуществлении Перевода денежных средств.

2.1.3. Информация, направляемая Оператору, предоставляется в следующие сроки:

- о статусе распоряжений о Переводе денежных средств – по запросу, согласно указанному в нем сроку, но не позднее 2-часов с момента отправления запроса;
- о выявленных нарушениях регламента функционирования Платежной системы, а также о зафиксированных Инцидентах, чрезвычайных и спорных ситуациях – незамедлительно, согласно порядку взаимодействия в рамках Платежной системы в спорных, нестандартных и чрезвычайных ситуациях;
- о данных, предоставляемых Оператору согласно требованиям нормативных актов Банка России, в т.ч. для формирования отчетности Банку России – на регулярной основе, в соответствии с п. 7.1 настоящих Правил.

2.1.4. При выявлении фактов нарушения Участниками, Расчетным центром и Оператором, в том числе действующим в качестве Операционного центра и Платежного клирингового центра обязательств, принятых на себя в соответствии с настоящими Правилами, Оператор осуществляет мероприятия, предусмотренные п.2.2 настоящих Правил.

2.2. Ответственность за несоблюдение Правил

2.2.1. Субъекты Платежной системы несут ответственность за неисполнение или ненадлежащее исполнение своих обязательств в соответствии с законодательством Российской Федерации, Правилами и договорами, заключенными между Субъектами Платежной системы.

2.2.2. В случае неисполнения Участником предусмотренных Правилами и договором участия обязательств, связанных с обеспечением достаточности денежных средств на Счете Участника для осуществления расчетов по операциям, совершенным Клиентами, а также в случае неисполнения обязательств по оплате оказанных услуг, указанных в Тарифах (Приложение № 2 к Правилам), Оператор вправе начислить пеню, а Участник обязан (в случае начисления) уплатить её в

размере 0,1% (Ноль целых одна десятая процента) от недостающей суммы за каждый день просрочки.

2.2.3. В случае неоднократного нарушения Участником Правил, Оператор вправе лишить организацию статуса Участника, расторгнув договор участия в одностороннем порядке с последующим уведомлением организации о расторжении договора участия.

2.2.4. В случае однократного неисполнения Участником предусмотренных Правилами и договором участия обязательств, связанных с обеспечением завершения расчетов, Оператор вправе лишить организацию статуса Участника, расторгнув договор участия в одностороннем порядке с последующим уведомлением организации о расторжении договора участия.

2.2.5. В случае сбоев в Платежной системе или наступления иных обстоятельств, повлекших излишнее перечисление, неперечисление или неполное перечисление денежных средств, связанных с работой в Платежной системе, Оператор обязуется в кратчайшие сроки устранить последствия таких сбоев или обстоятельств. Штрафные санкции со стороны, допустившей неперечисление, перечисление в неполном объеме или перечисление излишних денежных средств, вызванное вышеуказанными сбоями или обстоятельствами, не применяются.

2.2.6. Оператор несет ответственность за прямой ущерб, подтвержденный документально, причиненный Участникам или Расчетному центру вследствие несоблюдения Оператором настоящих Правил, неисполнения или ненадлежащего исполнения своих обязательств.

2.2.7. Оператор не несет ответственности за наступление неблагоприятных последствий для третьих лиц, включая Клиентов, возникших в результате ненадлежащего/несвоевременного исполнения обязательств Участником или Расчетным центром, предусмотренных Правилами и договорами/соглашениями.

2.2.8. Оператор и Расчетный центр не несут ответственности за нарушения в работе Платежной системы, произошедшие вследствие:

- неквалифицированного обслуживания или неисправности оборудования (в том числе каналов связи) Участников, третьих лиц, предназначенного для работы в Платежной системе;
- неквалифицированного использования Участниками, их сотрудниками программного обеспечения, предназначенного для использования в Платежной системе;
- неквалифицированных действий со стороны сотрудников Участника, взаимодействующих посредством автоматизированных рабочих мест, в том числе несанкционированного доступа неуполномоченных лиц к данным Платежной системы.

2.2.9. Операционный центр несет ответственность за реальный ущерб, причиненный Участникам и Расчетному центру вследствие неоказания (ненадлежащего оказания) операционных услуг в размере разовой неустойки, составляющей 0,03% от суммы неисполненных и/или исполненных с нарушением срока обязательств, за исключением случаев умышленного неоказания (ненадлежащего оказания) операционных услуг.

2.2.10. Платежный клиринговый центр несет ответственность за убытки, причиненные Участникам и Расчетному центру вследствие неоказания (ненадлежащего оказания) услуг платежного клиринга в размере разовой неустойки, составляющей 0,03% от суммы неисполненных и/или исполненных с нарушением срока обязательств, за исключением случаев умышленного неоказания (ненадлежащего оказания) услуг платежного клиринга.

2.2.11. 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 обязательства Субъекта разумными средствами, в том числе: землетрясения, наводнения, пожары,

эпидемии, аварии на транспорте, военные действия, массовые беспорядки и др. Субъект, подвергшийся действию обстоятельств непреодолимой силы и оказавшийся вследствие этого не в состоянии выполнить свои обязательства, должен незамедлительно, не позднее одного рабочего дня, сообщить о возникновении таких обстоятельств в письменной форме, в том числе в электронном виде по согласованным каналам связи, Оператору, в противном случае Субъект, 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.

2.3. Порядок изменения Правил

2.3.1. Изменения и/или дополнения в Правила вносятся Оператором в одностороннем порядке.

2.3.2. Для внесения изменений и/или дополнений в Правила Оператор обязан обеспечить Участникам возможность предварительного ознакомления с предлагаемыми изменениями и/или дополнениями. Возможность предварительного ознакомления с предлагаемыми изменениями и/или дополнениями обеспечивается путем размещения предлагаемых изменений и/или дополнений на Сайте Платежной системы.

2.3.3. Участники вправе предварительно ознакомиться с предполагаемыми изменениями и/или дополнениями в Правилах и направить свои предложения/замечания посредством использования Согласованного канала связи в срок не менее 1 (одного) месяца с момента размещения Правил на Сайте Платежной системы.

2.3.4. Изменения и/или дополнения в Правила вносятся в срок не менее одного месяца со дня окончания срока, указанного в п. 2.3.3 настоящих Правил.

2.3.5. Оператор обязан представлять в Банк России изменения и/или дополнения в Правила, изменения перечня Операторов услуг платежной инфраструктуры не позднее десяти дней со дня внесения соответствующих изменений.

2.3.6. Оператор оставляет за собой право использовать иные доступные средства информирования Участников.

2.4. Порядок раскрытия информации о Правилах

2.4.1. Оператор предоставляет организациям, намеревающимся участвовать в Платежной системе, Правила для предварительного ознакомления без взимания платы, за исключением расходов на изготовление копий Правил.

2.4.2. Правила, за исключением содержащейся в них информации о требованиях к защите информации и информации, доступ к которой ограничен в соответствии с Федеральным законом, являются публично доступными.

2.4.3. Правила размещаются на Сайте Платежной системы.

3. Оператор, Операторы услуг платежной инфраструктуры, Участники и их функции

Оператор совмещает свою деятельность с деятельностью Операционного центра и деятельностью Платежного клирингового центра.

3.1. Функции Оператора

3.1.1. Создает единое взаимодействие в Платежной системе, обеспечивает организационную и технологическую целостность Платежной системы, а также обеспечивает равноправный доступ Расчетных центров в Платежную систему.

3.1.2. Определяет Правила, организовывает и осуществляет контроль за их соблюдением Субъектами Платежной системы.

3.1.3. Осуществляет привлечение Расчетных центров, обеспечивает контроль за оказанием услуг платежной инфраструктуры, ведет перечень Операторов услуг платежной инфраструктуры.

3.1.4. Устанавливает требования (п. 3.4 настоящих Правил) к Расчетным центрам, с которыми могут заключаться договоры при их привлечении Оператором, в т.ч. в части их финансового состояния, технологического обеспечения.

3.1.5. Организует систему управления рисками в Платежной системе, осуществляет мониторинг, анализ, оценку и управление рисками в соответствии с требованиями законодательства Российской Федерации, нормативных актов Банка России и Правилами.

3.1.6. Обеспечивает прием и обработку обращений Участников по вопросам БФПС.

3.1.7. Обеспечивает досудебное и (или) третейское рассмотрение споров с Участниками и Операторами услуг платежной инфраструктуры в соответствии с Правилами.

3.1.8. Обеспечивает защиту информации о средствах и методах обеспечения информационной безопасности персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, в соответствии с требованиями к защите указанной информации, установленными Правительством Российской Федерации, в том числе защиту информации при осуществлении Переводов денежных средств в соответствии с требованиями, установленными Банком России, гарантирует защиту банковской тайны.

3.1.9. Указывает свой регистрационный номер при предоставлении информации о Платежной системе.

3.1.10. Устанавливает критерии и порядок участия в Платежной системе, а также случаи приостановления и/или прекращения участия в Платежной системе.

3.1.11. Поддерживает актуальность Правил и их соответствие требованиям действующего законодательства Российской Федерации и, в случае необходимости, в одностороннем порядке вносит изменения в Правила. Информирует Субъектов Платежной системы и Банк России о таких изменениях.

3.1.12. Приостанавливает и/или прекращает участие Участников в Платежной системе в порядке и по основаниям, установленными настоящими Правилами.

3.1.13. Информирует Банк России, Участников о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры в день такого приостановления (прекращения) путем размещения такой информации на сайте Платежной системы, а также в электронном виде по согласованным каналам связи, в соответствии с Правилами.

3.1.14. Обеспечивает БФПС в порядке, установленном Банком России.

3.1.15. Осуществляет взаимодействие с Участниками, в отношении которых Оператором получена информация о принятии уполномоченными государственными или иными регулирующими органами решений о приостановлении операций по счетам, о наложении ареста на денежные средства, размещенные на счетах, отзыве лицензии на осуществление банковских операций, иных обстоятельствах, препятствующих Участнику осуществлять Переводы денежных средств и, в установленных Правилами случаях и сроках, приостанавливает/прекращает, в соответствии с п. 5.4 настоящих Правил, участие данного Участника в Платежной системе.

3.1.16. Обеспечивает реализацию мероприятий в рамках Платежной системы (в том числе с привлечением операторов услуг платежной инфраструктуры) по противодействию осуществлению Переводов денежных средств без согласия Клиента в порядке, установленном Банком России.

3.1.17. Информирует Банк России обо всех случаях и (или) попытках осуществления Переводов денежных средств без согласия Клиента по форме и в порядке, которые установлены Банком России (в том числе с привлечением операторов услуг платежной инфраструктуры).

3.2. Требования к Операционному центру и его функции

3.2.1. Функции Операционного центра:

3.2.1.1. Обеспечивает в рамках Платежной системы для Участников и Клиентов доступ к услугам по Переводу денежных средств, а также обмен электронными сообщениями.

3.2.1.2. Обеспечивает маршрутизацию авторизационных сообщений, передаваемых в режиме реального времени между Участниками, между Участниками и Платежным клиринговым центром, между Платежным клиринговым центром и Расчетным центром.

3.2.1.3. Обеспечивает передачу извещения (подтверждения) о приеме и об исполнении распоряжений Участников.

3.2.1.4. Обеспечивает регистрацию Участников в Платежной системе.

3.2.1.5. Обеспечивает обмен информацией, не являющейся финансовыми сообщениями.

3.2.1.6. Обеспечивает защиту обрабатываемой в соответствии с выполняемыми функциями Операционного центра информации о Переводах денежных средств.

3.2.1.7. Не раскрывает третьим лицам сведения об операциях и о Счетах Участников и их Клиентов, полученные при оказании операционных услуг, за исключением передачи информации в рамках Платежной системы, а также случаев, предусмотренных федеральными законами.

3.2.1.8. Выполняет иные функции, связанные с использованием информационно-коммуникационных технологий, необходимые для функционирования Платежной системы, в соответствии с настоящими Правилами.

3.2.2. Требования к Операционному центру:

- организация имеет технологическую возможность подключения к ПС;
- организация обязуется обеспечивать поддержание уровня бесперебойности оказания операционных услуг в рамках Платежной системы в соответствии с Правилами.

3.3. Требования к Платежному клиринговому центру и его функции

3.3.1. Функции Платежного клирингового центра:

3.3.1.1. Обеспечивает в рамках Платежной системы прием к исполнению распоряжений Участников об осуществлении Перевода денежных средств. Осуществляет проверку соответствия распоряжений Участников установленным требованиям.

3.3.1.2. Формирует и передает Расчетному центру на исполнение распоряжения на сумму платежных клиринговых позиций на нетто-основе Участников в соответствии с установленным Временным регламентом (Реестр нетто позиций).

3.3.1.3. Определяет Платежные клиринговые позиции на нетто-основе.

3.3.1.4. Рассчитывает вознаграждения за услуги, оказываемые Участниками и Операционным центром.

3.3.1.5. Направляет Участникам извещения (подтверждения), касающиеся приема и исполнения распоряжений.

3.3.1.6. Отказывает в приеме платежного распоряжения Участника при отрицательных результатах контроля процедур приема к исполнению.

3.3.1.7. Выполняет иные функции в соответствии с настоящими Правилами.

3.3.2. Требования к Платежному клиринговому центру:

- организация имеет технологическую возможность подключения к ПС;
- организация обязуется обеспечивать поддержание уровня бесперебойности оказания операционных услуг в рамках Платежной системы в соответствии с Правилами.

3.4. Требования к Расчетному центру и его функции

Правила являются неотъемлемой частью договора оказания услуг между Оператором и Расчетным центром.

3.4.1. Требования к Расчетному центру:

3.4.1.1. Расчетным центром Платежной системы может выступать Банк России или кредитная организация, созданная в соответствии с законодательством Российской Федерации, в том числе

небанковская кредитная организация, находящаяся на территории Российской Федерации, осуществляющая не менее одного года деятельность по переводу денежных средств по распоряжению юридических лиц, в том числе Прямых Участников, по открытым в этой кредитной организации банковским счетам.

3.4.1.2. Расчетный центр должен соответствовать следующим требованиям к финансовому состоянию, а также другим факторам, влияющим на БФПС:

- наличие лицензии Банка России и иных правоустанавливающих документов (учредительные документы, сертификаты и т.п.), необходимых для осуществления соответствующей деятельности кредитной организации согласно действующему законодательству Российской Федерации;
- кредитная организация не менее одного года осуществляет перевод денежных средств по открытым в этой кредитной организации банковским счетам;
- финансовая устойчивость, определяемая с учетом соответствия обязательных нормативов и иных экономических показателей требованиям Банка России;
- поддержание уровня бесперебойности оказания расчетных услуг в рамках Платежной системы в соответствии с Правилами.

3.4.1.3. Расчетный центр выполняет обязательные требования Банка России, в том числе требования по обеспечению мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма.

3.4.1.4. Расчетный центр обеспечивает банковскую тайну, защиту информации при осуществлении Переводов денежных средств и персональных данных Отправителей (в случае их получения и обработки) в соответствии с законодательством Российской Федерации.

3.4.1.5. Расчетный центр имеет технологическую возможность быть подключенным к Платежной системе.

3.4.1.6. Расчетный центр не вправе в одностороннем порядке приостанавливать (прекращать) оказание расчетных услуг Участникам в Платежной системе.

3.4.1.7. Расчетный центр осуществляет свою деятельность в соответствии с нормативными актами Банка России, Правилами и на основании договора, заключаемого с Оператором, а также на основании договоров банковского счета с Участниками, используемых для расчетов по операциям Платежной системы.

3.4.2. Функции Расчетного центра.

Расчетный центр обеспечивает в рамках Платежной системы в соответствии с Временным регламентом:

- исполнение распоряжений Платежного клирингового центра посредством списания и/или зачисления денежных средств по Счетам Прямых Участников;
- направление подтверждения (извещения), касающегося исполнения распоряжений Платежного клирингового центра;
- предоставление данных по остаткам/изменениям денежных средств на Счетах Прямых Участников для осуществления контроля за рисками неисполнения (ненадлежащего исполнения) Прямыми Участниками своих обязательств по расчетам в рамках Платежной системы;
- предоставление Оператору по его запросу отчетов, любой информации, связанной с осуществлением Расчетным центром, возложенных на него в рамках Платежной системы функций и соблюдением требований, изложенных в Правилах;
- выполнение иных функций в соответствии с настоящими Правилами.

3.5. Функции Участника

Платежная система предусматривает прямое и косвенное участие. Прямое участие в Платежной системе требует открытия в Расчетном центре Счета Прямого Участника в целях осуществления расчета с другими Участниками. Косвенное участие предполагает открытие Счета Косвенного Участника у Прямого Участника.

3.5.1. Обеспечивает взаимодействие с Операционным центром для получения информации о финансовых сообщениях в соответствии с особенностями осуществления платежного клиринга, предусмотренного настоящими Правилами.

3.5.2. Несет обязательства по зачислению денежных средств на счет Получателей в срок не превышающий 1 (один) рабочий день с момента получения распоряжения от Платежного клирингового центра.

3.5.3. Оплачивает услуги согласно Тарифам Платежной системы, предоставляемые Операторами услуг платежной инфраструктуры.

3.5.4. Открывает Счет Участника в Расчетном центре/у Прямого Участника. Контролирует достаточность денежных средств на Счете Участника для осуществления Переводов.

3.5.5. Незамедлительно информирует Оператора о любых обстоятельствах, которые могут повлиять на исполнение Участником своих обязательств.

3.5.6. Обеспечивает получение согласия на обработку (включая автоматизированную обработку) идентификационных данных Клиентов.

3.5.7. Выполняет требования по обеспечению безопасности в Платежной системе в соответствии с Правилами.

3.5.8. В случае внесения изменений в учредительные документы, а также при изменении других данных Участника, предоставляет указанные изменения Оператору не позднее десяти рабочих дней с даты их государственной регистрации.

3.5.9. Самостоятельно разрабатывает свою методику анализа рисков в Платежной системе и предоставляет ее Оператору по мере внесения изменений, но не реже одного раза в три года.

3.5.10. Взимает с Отправителей комиссионное вознаграждение за оказываемые Услуги в рамках Платежной системы.

4. Порядок взаимодействия Субъектов Платежной системы

4.1. Общие положения

4.1.1. Участник вправе оказывать Услуги в рамках Платежной системы на условиях, предусмотренных Правилами и договором, заключенным с Оператором.

4.1.2. Операции по Переводу денежных средств в Платежной системе совершаются Отправителями через пункты обслуживания Банка-Отправителя, посредством ДБО Участника и (или) Мобильного приложения.

4.1.3. Расчеты по Переводам, совершаемым в рамках Платежной системы Отправителями, осуществляются через Счета Прямых Участников, открытые в Расчетном центре, а также через Счета Косвенных Участников, открытых у Прямых Участников.

4.2. Взаимодействие Оператора с Участниками

4.2.1. Взаимодействие между Оператором и Участником осуществляется с момента выражения намерения потенциального Участника присоединиться к Правилам (выражением намерения является направление Заявление на участие в Платежной системе «МОМЕНТОМ» (Приложение № 1 к Правилам), далее в рамках подписания договора участия в Платежной системе и открытия Счета Прямого Участника в Расчетном Центре/открытие Счета Косвенного Участника у Прямого Участника) в качестве Участника, и в дальнейшем в процессе осуществления им функций Участника вплоть до момента прекращения указанной деятельности последнего.

4.2.2. При получении Оператором информации о принятии уполномоченными государственными или иными регулирующими органами решений о приостановлении операций по

Счету Участника, о наложении ареста на денежные средства, размещенные на Счете Участника, отзыве лицензии на осуществление банковских операций, а так же в случаях, предусмотренных п. 5.4.2 настоящих Правил и иных обстоятельствах, препятствующих Участнику осуществлять Перевод денежных средств, Оператор незамедлительно информирует Участника уведомлением о данных обстоятельствах по Согласованным каналам связи.

4.2.3. При непоступлении (в течение двух часов с момента отправления уведомления, указанного в п. 4.2.2 настоящих Правил) от Участника сведений, подтверждающих отсутствие ограничений, Оператор, действуя в качестве Платежного клирингового центра, приостанавливает операции Участника. В этом случае, возникшие обстоятельства рассматриваются как обстоятельства непреодолимой силы и выполняются мероприятия, предусмотренные п. 5.4.3 настоящих Правил.

4.2.4. Принимаемые Оператором решения об участии, приостановлении и прекращении участия в Платежной системе Участника направляются в адрес Участника посредством использования Согласованного канала связи не позднее рабочего дня, следующего за днем принятия Оператором такого решения. Также Оператор уведомляет других Участников и ОУПИ о принятом решении по согласованным каналам связи в срок, не позднее рабочего дня, следующего за днем принятия Оператором такого решения.

4.3. Взаимодействие Оператора и Расчетного центра

4.3.1. Взаимодействие Расчетного центра с Оператором, в том числе по вопросам защиты информации, обеспечения БФПС, управления рисками, а также по иным вопросам осуществляется в соответствии с Правилами и на условиях договора, заключаемого между Расчетным центром и Оператором посредством использования Согласованных каналов связи.

4.4. Взаимодействие Расчетного центра и Прямого Участника

4.4.1. Прямому Участнику на условиях договора, заключаемого между Прямым Участником и Расчетным центром, открывается Счет Участника.

4.4.2. Договор счета между Расчетным центром и Прямым Участником заключается после присоединения Участника к Правилам, по факту предоставления Участником в адрес Расчетного центра копии договора участия в Платежной системе.

4.5. Взаимодействие Оператора с Партнерами

4.5.1. Партнеры не присоединяются к Правилам ПС в целях осуществления Переводов денежных средств.

4.5.2. Взаимодействие осуществляется в рамках отдельно существующего соглашения/договора, заключенного с Оператором. Условия такого договора определяют следующие области взаимодействия:

а) размер и порядок оплаты вознаграждения сторон договора;

б) условия проведения клиринга взаиморасчетов сторон договора;

в) порядок электронного документооборота;

г) особенности Переводов денежных средств, при осуществлении которых задействован Партнер;

д) иные особенности взаимодействия сторон договора.

4.5.3. Переводы денежных средств, осуществленных посредством применения таких договоров, имеют следующие особенности:

а) окончательность Перевода денежных средств наступает в момент зачисления денежных средств на банковский счет Партнера, если иное не содержится в договоре между Оператором и Партнером;

б) возможность или невозможность внесения изменений в Перевод денежных средств определяется каждый раз Партнером, при получении соответствующего запроса от Оператора. При получении информации от Партнера о невозможности внесения изменений в Перевод

денежных средств, Оператор, в свою очередь, посредством Согласованных каналов уведомляет Участника, обслуживающего Отправителя;

в) возможность или невозможность возврата Перевода денежных средств определяется каждый раз Партнером, при получении соответствующего запроса от Оператора. При получении информации от Партнера о невозможности осуществления возврата Перевода денежных средств, Оператор, в свою очередь, посредством Согласованных каналов уведомляет Участника, обслуживающего Отправителя.

4.5.4. Информирование Участников о существующих особенностях (в том числе ограничениях) при Переводе денежных средств через Партнеров, Оператор осуществляет с использованием Согласованных каналов.

5. Порядок присоединения и участия в Платежной системе субъектов Платежной системы

5.1. Порядок привлечения Операторов услуг платежной инфраструктуры, ведение перечня Операторов услуг платежной инфраструктуры

5.1.1. В рамках Платежной системы функции Операционного центра и Платежного клирингового центра выполняет Оператор. При этом, Оператор оставляет за собой право и возможность привлечения Операционного центра на условиях равноправного доступа при соответствии требованиям, указанным в п.3.2.3 настоящих Правил и на основании соответствующего договора. В Платежной системе может быть несколько Операционных центров.

5.1.2. Расчетный центр привлекается Оператором на условиях равноправного доступа при соответствии требованиям, указанным в п. 3.4.1 настоящих Правил и на основании договора о предоставлении услуг Расчетного центра, заключенного между Расчетным центром и Оператором. В Платежной системе может быть несколько Расчетных центров.

5.1.3. Ведение перечня Операторов услуг платежной инфраструктуры осуществляется Оператором самостоятельно путем включения в него информации об Операторе услуг платежной инфраструктуры.

5.1.4. Оператор поддерживает перечень Операторов услуг платежной инфраструктуры в актуальном состоянии:

- перечень Операторов услуг платежной инфраструктуры публикуется на Сайте Платежной системы;
- при любом изменении перечня Операторов услуг платежной инфраструктуры Оператор в течение 5 (Пяти) рабочих дней с момента возникновения оснований для внесения изменений вносит изменения в перечень;
- Оператор представляет в Банк России новую редакцию перечня Операторов услуг платежной инфраструктуры не позднее 10 (Десяти) дней со дня внесения соответствующих изменений.

5.2. Критерии участия Участников в Платежной системе

5.2.1. Для Прямых Участников предусмотрены следующие критерии участия в Платежной системе:

- наличие договора участия, заключенного с Оператором;
- наличие Счета (Счетов) в Расчетном центре.

5.2.2. Для Косвенных Участников предусмотрены следующие критерии участия в Платежной системе:

- наличие договора участия, заключенного с Оператором;
- наличие Счета (Счетов) у Прямого Участника.

5.2.3. Организация может присоединиться к Платежной системе при удовлетворении такой организации следующим критериям:

- финансовая устойчивость юридического лица (в т.ч.ненахождение в стадии ликвидации, банкротства или наблюдения);
- наличие действующей лицензии на право осуществления переводов денежных средств (в отношении кредитных организаций, в том числе иностранных);
- наличие технической возможности интеграции в Платежную систему;
- наличие доступа к сети Интернет;
- соблюдение обязательных нормативов Банка России (в отношении кредитных организаций – резидентов Российской Федерации);
- соблюдение требований законодательства Российской Федерации по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (в отношении организаций – резидентов Российской Федерации);
- обеспечение защиты информации в собственных информационных системах, а также при взаимодействии с Операторами услуг платежной инфраструктуры, в соответствии с требованиями законодательства Российской Федерации, нормативных актов Правительства Российской Федерации и Банка России, Правил (в отношении организаций – резидентов Российской Федерации).

5.2.4. Присоединение организации к Платежной системе является бесплатным.

5.3. Порядок присоединения организации к Платежной системе

5.3.1. Для получения статуса Участника организация, отвечающая критериям, установленным в п. 5.2 настоящих Правил, направляет Оператору заявление на участие в Платежной системе, согласно форме Приложения № 1. Вместе с заявлением предоставляется пакет документов в соответствии с перечнем, утвержденным Оператором (установлено п. 7 Приложения № 1 к Правилам). Оператор имеет право запросить у организации, направившей заявление на участие, дополнительные документы и сведения для принятия решения о присоединении такой организации в качестве Участника.

5.3.2. В случае принятия Оператором положительного решения о включении организации в число Участников, ей направляется договор об участии, а также иные сопутствующие документы. Организация присоединяется к Правилам путем принятия их в целом. При отрицательном решении Оператора организации направляется только уведомление, содержащее информацию об отказе.

5.3.3. Оператор отказывает в присвоении статуса Участника в случае несоответствия организации требованиям действующего законодательства Российской Федерации, Правил и/или не предоставления документов, запрошенных Оператором.

5.3.4. Датой начала участия организации в Платежной системе является:

- для Прямых Участников: дата открытия Счета Участника в Расчетном центре;
- для Косвенных Участников: дата открытия Счета Участника у Прямого Участника.

5.4. Критерии приостановления и прекращения участия в Платежной системе

5.4.1. В случае несоблюдения Участником условий, установленных Правилами, Оператор вправе до даты устранения Участником допущенного нарушения в одностороннем порядке приостановить его участие в Платежной системе, а именно: приостановить возможность совершения Перевода денежных средств Клиентами, а также ограничить в иных правах и не оказывать иные услуги, предусмотренные Правилами.

5.4.2. Оператор вправе приостановить участие в Платежной системе Участника в случаях:

- нарушения и/или несоблюдения Участником Правил;
- отказа в предоставлении Оператору Участником о своей деятельности или иных сведений по запросу Оператора;
- невыполнения Участником критериев участия в Платежной системе;

- несоблюдения Участником требований к защите информации, вследствие которых нанесен ущерб другому Участнику(ам) и/или Оператору, или создана существенная угроза нанесения такого ущерба;
- имеющихся в распоряжении Оператора сведений, позволяющих сделать вывод о высокой вероятности возникновения рисков, ведущих к невозможности осуществления расчетов по операциям, совершенным Клиентами Участника, в том числе неисполнения обязанности по обеспечению достаточности денежных средств на Счете Участника;
- приостановления или отмены полномочий Участника компетентными органами власти, или выпуск уведомления о своем намерении поступить таким образом;
- приостановления государственным органом операций Участника или наложения ареста на денежные средства Участника, находящиеся на Счете(ах) в Расчетном центре.

5.4.3. Оператор не позднее рабочего дня, следующего за днем приостановления участия, по Согласованному каналу связи уведомляет Участника о причинах приостановления участия и о необходимости устранения Участником допущенных нарушений. После устранения Участником допущенных нарушений и их последствий участие Участника в Платежной системе возобновляется по письменному заявлению Участника с приложением документов, подтверждающих устранение допущенных нарушений и их последствий.

5.4.4. Участие в Платежной системе Участника прекращается по инициативе Оператора в следующих случаях:

- невозможности со стороны Участника устранить нарушения Правил в течение одного месяца с даты выявления таких нарушений;
- отзыва у Участника необходимых для его деятельности в рамках Платежной системы разрешений (лицензии), либо приостановления их действия;
- объявления Участником о своей ликвидации, либо инициирования в отношении него процедуры банкротства;
- несоблюдения Участником требований к защите информации, вследствие которых нанесен ущерб Субъектам Платежной системы или создана существенная угроза нанесения такого ущерба;
- невыполнения Участником мер по противодействию легализации денежных средств, полученных преступным путем и финансированию терроризма;
- невыполнения требований настоящих Правил по обеспечению БФПС, вследствие чего может быть нанесен существенный ущерб Субъектам Платежной системы.

5.4.5. Договор участия считается расторгнутым с даты прекращения участия Участника в Платежной системе.

5.4.6. Участник может прекратить свое участие в Платежной системе путем направления Оператору не менее чем за тридцать календарных дней до предполагаемой даты прекращения участия заявления о прекращении участия в Платежной системе, составленного в письменной форме на бумажном носителе, подписанного уполномоченным лицом Участника и скрепленного печатью Участника. Не позднее третьего рабочего дня со дня получения заявления о прекращении участия Оператор приостанавливает участие Участника в Платежной системе. Оператор уведомляет Участника об объеме неисполненных обязательств Участника, связанных с участием в Платежной системе. Участник обязан не позднее одного рабочего дня с даты получения уведомления от Оператора осуществить расчеты по всем своим обязательствам. Участие Участника в Платежной системе прекращается со дня, указанного в заявлении о прекращении участия в Платежной системе, согласованного с Оператором и при выполнении всех расчетов по своим обязательствам в рамках Платежной системы. Оператор уведомляет Участника о прекращении его участия в Платежной системе в письменной форме посредством использования Согласованного канала связи не позднее

рабочего дня, следующего за днем прекращения участия Участника в Платежной системе. Также Оператор уведомляет других Участников и ОУПИ о прекращении участия Участника в Платежной системе по согласованным каналам связи в срок, не позднее рабочего дня, следующего за днем прекращения участия Участника в Платежной системе.

5.5. Порядок присвоения Участнику идентификационного кода (номера)

5.5.1. Участнику присваивается идентификационный цифровой (шестиразрядный) порядковый номер, который представляет собой порядковый номер Участника в реестре Участников Платежной системы и вид его участия.

5.5.2. Идентификационный код присваивается Оператором автоматически.

5.5.3. В случае если Участник выходит из состава Участников Платежной системы, его номер не присваивается новому Участнику.

6. Порядок осуществления Перевода денежных средств в рамках Платежной системы

6.1. Применяемые формы безналичных расчетов

6.1.1. Переводы денежных средств в Платежной системе осуществляются в форме безналичных расчетов - расчетов платежными поручениями.

6.1.2. Основанием для осуществления Переводов денежных средств являются распоряжения Отправителей, принятые к исполнению Банком-Отправителем для Перевода в Платежной системе согласно заключенному договору Банковского счета, а также платежные поручения по собственным операциям Банка-Отправителя.

6.1.3. Для осуществления трансграничных переводов Оператором могут быть использованы иные формы в соответствии с заключенными соглашениями/договорами с Партнерами.

6.2. Осуществление Перевода денежных средств в рамках Платежной системы, включая моменты наступления его безотзывности, безусловности и окончательности

6.2.1. Перевод денежных средств в Платежной системе осуществляется на основании распоряжения Банка–Отправителя, составленного в соответствии с распоряжением Отправителя.

6.2.2. Распоряжения Банка-Отправителя принимаются и исполняются путем реализации процедур приема к исполнению и процедур исполнения согласно требованиям нормативных актов Банка России с учетом особенностей платежного клиринга и расчетов Платежной системы, в том числе предусмотренных настоящими Правилами.

6.2.3. Сопровождение Перевода денежных средств сведениями об Отправителе осуществляется Участником в соответствии с требованиями Федерального закона № 115-ФЗ в случае, если они не содержатся в распоряжении Участника. Участники реализуют комплекс мероприятий, направленных на предотвращение легализации (отмывания) доходов, полученных преступным путем, и финансированию терроризма.

6.2.4. Безотзывность Перевода наступает в момент списания денежных средств с Банковского счета Отправителя.

6.2.5. Переводы являются безусловными, т.к. в Правилах отсутствуют дополнительные условия осуществления Перевода.

6.2.6. Окончательность Перевода наступает в момент зачисления денежных средств на Счет Банка-Получателя.

6.3. Порядок осуществления платежного клиринга

6.3.1. Распоряжение Банка Отправителя принимается к исполнению Платежным клиринговым центром для осуществления дальнейшей обработки распоряжения Участника согласно Временного регламента и с учетом особенностей платежного клиринга, установленного настоящими Правилами.

6.3.2. Определение платежной клиринговой позиции Прямого Участника осуществляется на нетто-основе с учетом применения тарифов и согласно Временному регламенту.

6.3.3. При определении платежной клиринговой позиции Прямого Участника учитываются платежные клиринговые позиции Косвенных Участников, находящихся на расчетном обслуживании такого Прямого Участника. При этом, в составе нетто-позиции Прямого Участника не учитываются Переводы денежных средств Косвенных Участников, если они одновременно обслуживаются у одного Прямого Участника.

6.3.4. Платежный клиринговый центр предоставляет информацию о текущей платежной клиринговой позиции Косвенного Участника Прямому Участнику, у которого открыты счета данного Косвенного Участника, для осуществления расчетов с Расчетным центром.

6.3.5. В целях обеспечения исполнения обязательств Прямых Участников для каждого такого Участника устанавливаются лимиты межбанковских расчетов, соответствие которым контролируется Платежным клиринговым центром при приеме распоряжений Участников. Лимиты автоматически устанавливаются Платежным клиринговым центром в начале операционного дня в размере остатка денежных средств на Счете Участника для каждого Прямого Участника и могут в дальнейшем изменяться в течение операционного дня. Размер лимита расчетов для Прямого Участника контролируется и устанавливается Платежным клиринговым центром.

6.3.6. При приеме Платежным клиринговым центром к исполнению каждого распоряжения Участника (осуществляется круглосуточно), включая проверку соответствия распоряжения Участника установленным требованиям, определяются (корректируются) текущие платежные клиринговые позиции Участников, вычисляемые на нетто-основе (как разница между общей суммой подлежащих исполнению распоряжений Участников, по которым Участник является Банком-Отправителем, и общей суммой распоряжений Участников, по которым Участник является Банком-Получателем).

6.3.7. При контроле Платежным клиринговым центром достаточности денежных средств определяется разница между лимитом и текущей платежной клиринговой позицией каждого Участника:

- при отрицательной разнице распоряжение Участника помещается в состав распоряжений, ожидающих исполнения (далее - очередь распоряжений, ожидающих исполнения – Стоп лист);
- при положительной разнице распоряжение Участника включается в состав принятых распоряжений, подлежащих исполнению.

6.3.8. В период завершения приёма распоряжений к обработке текущим операционным днем, предусмотренным Временным регламентом (глава 9 настоящих Правил), осуществляются следующие действия:

- Платежный клиринговый центр оформляет платежное распоряжение на сумму каждой платежной клиринговой позиции, вычисленной на нетто-основе, согласно требованиям нормативных актов Банка России и направляет Реестр нетто-позиций для исполнения в Расчетный центр;
- Расчетный центр по результатам исполнения направляет в Платежный клиринговый центр сообщение, подтверждающее списания и зачисления денежных средств по счетам Прямых Участников в размере платежных клиринговых позиций;
- Платежный клиринговый центр направляет Участникам сообщения с подтверждением исполнения распоряжений, согласно платежным клиринговым позициям, а также об аннулированных распоряжениях (в том числе из Стоп-листа);
- списания и зачисления денежных средств по счетам Прямых Участников осуществляется Расчетным центром текущим рабочим днем;
- в случае приостановления операций Участника, Платежный клиринговый центр с момента уведомления осуществляет отказ в приеме распоряжений Участника. Возникшие

обстоятельства рассматриваются как обстоятельства непреодолимой силы и выполняются мероприятия, предусмотренные п. 5.4.3 настоящих Правил.

6.4. Порядок осуществления расчетов в Платежной системе Прямых Участников

6.4.1. Расчеты в ПС могут осуществляться в российских рублях, долларах США, ЕВРО и /или национальных валютах стран Участников/Партнеров. Расчеты с использованием конвертации осуществляются в соответствии с п.9.3 настоящих Правил.

6.4.2. Расчеты осуществляются по Счетам Прямых Участников. Прямой Участник размещает на своем Счете Участника, денежные средства в размере, достаточном для обеспечения расчетов по операциям, инициированным Клиентами Прямого Участника, в том числе Клиентами Косвенного Участника.

6.4.3. Порядок и условия открытия Счетов Прямых Участников определяются Расчетным центром и не являются предметом регулирования настоящих Правил. В случае любых несоответствий между настоящими Правилами и договором между Прямым Участником и Расчетным центром преимущественную силу имеют положения Правил.

6.4.4. Прямой Участник предоставляет Расчетному центру право на основании заранее данного акцепта списывать со Счета Прямого Участника денежные суммы для проведения расчетов в рамках Платежной системы.

6.4.5. Расчеты с Косвенными Участниками Прямые Участники, у которых находятся на расчетном обслуживании соответствующие Косвенные Участники, осуществляют самостоятельно в соответствии с Реестром нетто-позиций, сформированным и полученным от Платежного клирингового центра.

6.5. Особенности расчетов с Косвенными Участниками через Счета Прямых Участников

6.5.1. Расчеты с Косвенными Участниками осуществляются по Счетам Прямых Участников.

6.5.2. Расчеты по операциям Косвенных Участников осуществляются по Счетам Прямых Участников на основании определенной на нетто-основе платежной клиринговой позиции каждого Косвенного Участника.

6.5.3. Прямой Участник, в случае открытия у него Счетов Косвенных Участников, обязан:

- включать в свои договоры (в том числе договоры банковского счета) с Косвенными Участниками положения, обеспечивающие выполнение требований настоящего Раздела Правил;
- поддерживать на Счете Прямого Участника, остатки денежных средств, достаточные для осуществления своевременных и бесперебойных расчетов, как по собственным операциям, так и по операциям Косвенных Участников;
- обеспечить окончательные расчеты с Косвенными Участниками на основании информации из Реестра нетто-позиций не позднее следующего операционного дня после осуществления расчетов Расчетным центром при условии достаточности средств на Счетах Косвенных Участников.

6.6. Порядок обеспечения исполнения обязательств Участников по Переводу денежных средств

6.6.1. Обязательства Участников по Переводу денежных средств в рамках Платежной системы исполняются за счет средств Прямых Участников, находящихся на их Счетах Участников.

6.6.2. Расчетный центр осуществляет исполнение обязательств Участника (в том числе и Косвенного Участника, находящегося на расчетном обслуживании у данного Прямого Участника) в пределах остатка денежных средств на Счете Прямого Участника на момент проведения расчетов.

Расчетный центр несет ответственность за своевременное оказание расчетных услуг Платежной системы в рамках установленных лимитов.

6.6.3. Установка лимита расчетов Прямого Участника осуществляется на основании информации от Расчетного центра об остатках денежных средств на Счете Прямого Участника.

6.6.4. Прямой Участник поручает Расчетному центру предоставлять Платежному клиринговому центру, данные об остатках на Счете такого Участника и/или каждый раз в случае изменения остатка денежных средств.

6.6.5. Прямой Участник размещает на своем Счете Участника необходимую сумму денежных средств для проведения расчетов.

6.6.6. Для обеспечения исполнения обязательств Участников Оператор вправе установить следующую форму контроля – создание Гарантийного фонда ПС.

6.6.7. В случае создания Гарантийного фонда ПС, Оператор поручает ответственному Расчетному центру открытие и ведение счета Гарантийного фонда Платежной системы.

6.6.8. Гарантийный фонд ПС формируется для обеспечения обязательств Платежной системы по трансграничным переводам.

6.6.9. Оператор формирует Гарантийный фонд за счет собственных средств и/или средств Участников/Партнеров, при оказании Услуг ПС по трансграничным переводам.

6.7. Порядок оплаты услуг по Переводу денежных средств и услуг платежной инфраструктуры

6.7.1. Порядок оплаты услуг по Переводу денежных средств, услуг платежной инфраструктуры и услуг Оператора в рамках Платежной системы являются едиными и единообразными для всех Участников (Приложение № 2 к Правилам).

6.7.2. Услуги Оператора, выполняющего функции Операционного центра и Платежного клирингового центра, предоставляемые в рамках Платежной системы, Участники оплачивают в соответствии с Тарифами Оператора (Приложение № 2 к Правилам).

6.7.3. Запрещено устанавливать минимальный размер оплаты услуг по Переводу денежных средств Участниками и их Клиентами.

6.7.4. Оператор вправе вносить изменения в стоимость услуг и порядок их оплаты в порядке, предусмотренном для внесения изменений в Правила.

7. Порядок предоставления Участниками и Операторами услуг платежной инфраструктуры информации о своей деятельности Оператору

7.1. Используя Согласованный канал связи, Участники и Расчетный центр, предоставляют отчетность:

- форма № 0409101 «Оборотная ведомость по счетам бухгалтерского учета кредитной организации». Отчетность предоставляется Оператору в электронном виде/на бумажном носителе, надлежаще оформленная, не позднее десятого рабочего дня с даты, установленной законодательством для предоставления данной отчетности;
- форма № 0403203 "Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств" ежеквартально не позднее десятого рабочего дня месяца, следующего за отчетным кварталом;
- по запросу Оператора предоставляется надлежаще оформленная отчетность по форме № 0409102 «Отчет о финансовых результатах кредитной организации» в электронном виде/на бумажном носителе не позднее десятого рабочего дня с даты, установленной законодательством для предоставления данной отчетности.

В случае публикации отчетности на официальном сайте кредитной организации и/или официальном сайте Банка России информация об этом доводится до Оператора, при этом отчетность не предоставляется.

В случае если отчетность по форме № 0403203 "Сведения о событиях, связанных с нарушением защиты информации при осуществлении переводов денежных средств" содержит нулевые сведения, то Участники и Расчетный центр имеют право не предоставлять Оператору в указанные сроки данную форму.

7.2. Дополнительно, по запросу Оператора Участники и Расчетный центр обязаны в срок, не превышающий пяти рабочих дней со дня получения указанного запроса, предоставлять Оператору информацию о своей деятельности, связанную с оказанием услуг, предусмотренных Правилами, а также связанную с выполнением возложенных на них функций и обязанностей в рамках Платежной системы.

7.3. Требования настоящего раздела относятся к организациям – резидентам Российской Федерации. В случае, если Участником является иностранная организация, то Оператор вправе запрашивать отчетность/сведения о деятельности такого Участника в соответствии с национальным законодательством страны инкорпорации Участника раскрывающие следующие показатели:

- размер уставного капитала или собственных средств Участника;
- соблюдение обязательных нормативов, установленных национальным (центральным) банком страны инкорпорации Участника;
- осуществление мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, установленных ФАТФ, действующим законодательством страны инкорпорации Участника в области противодействия (легализации) доходов, полученных преступным путем, и финансирования терроризма;
- соблюдение требований по защите информации при осуществлении Переводов согласно законодательству страны инкорпорации такого Участника;
- обеспечение банковской тайны и защиты персональных данных в соответствии с законодательством Российской Федерации и страны инкорпорации такого Участника.

8. Порядок обеспечения бесперебойности функционирования Платежной системы, система управления рисками в Платежной системе

8.1. Требования к Оператору при обеспечении БФПС

8.1.1. При обеспечении БФПС, которая достигается при условии оказания Участникам Платежной системы УПИ согласно требованиям к оказанию услуг и (или) восстановления оказания УПИ, соответствующего требованиям к оказанию услуг в течение 6 часов и восстановления оказания УПИ в случае приостановления их оказания в течение 6 часов, к Оператору применяются требования, определенные в настоящем разделе.

8.1.2. Оператор обеспечивает БФПС путем осуществления скоординированной с Операторами УПИ и Участниками Платежной системы «МОМЕНТОМ» деятельности:

- по управлению рисками в Платежной системе «МОМЕНТОМ»;
- по управлению непрерывностью функционирования Платежной системы «МОМЕНТОМ».

8.2. Требования к порядку обеспечения БФПС

8.2.1. Оператор определяет и соблюдает порядок обеспечения БФПС, который включает:

- управление рисками в Платежной системе;
- управление непрерывностью функционирования Платежной системы;
- организацию взаимодействия Субъектов Платежной системы по обеспечению БФПС;
- контроль за соблюдением Операторами УПИ и Участниками порядка обеспечения БФПС.

8.3. Управление рисками в Платежной системе

8.3.1. Оператор организует систему управления рисками в Платежной системе «МОМЕНТОМ» с учетом организационной модели управления рисками в Платежной системе, определенной в соответствии с требованиями части 2 статьи 28 Закона о НПС.

Под системой управления рисками в Платежной системе понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для БФПС с учетом размера причиняемого ущерба.

В качестве организационной модели управления рисками в Платежной системе принята модель, предусматривающая распределение функций по оценке и управлению рисками между Оператором, Операторами УПИ и Участниками.

8.3.2. Оператор определяет собственную структуру управления рисками и функциональные обязанности лиц в соответствующих структурных подразделениях, ответственных за управление рисками.

8.3.3. По осуществлению управления рисками устанавливается разграничение ответственности и полномочий между Субъектами Платежной системы.

8.3.4. Оператор определяет следующие основные права, обязанности и функции Субъектов Платежной системы по управлению рисками, управлению непрерывностью функционирования Платежной системы, порядку взаимодействия и контроля Оператором соблюдения Операторами УПИ и Участниками порядка обеспечения БФПС.

8.3.4.1. Оператор:

- организует систему управления рисками в Платежной системе «МОМЕНТОМ»;
- проводит оценку рисков в Платежной системе «МОМЕНТОМ»;
- определяет способы управления рисками;
- определяет показатели БФПС;
- определяет мероприятия по управлению рисками;
- осуществляет анализ рисков нарушения БФПС на основании первичной информации, предоставляемой Субъектами Платежной системы;
- устанавливает допустимый уровень риска нарушения БФПС;
- выявляет текущие изменения присущего уровня риска нарушения БФПС;
- принимает меры, необходимые для достижения или поддержания допустимого уровня рисков нарушения БФПС;
- устанавливает и пересматривает пороговые уровни показателей БФПС;
- рассчитывает и анализирует значения показателей БФПС;
- проводит оценку системы управления рисками;
- вносит изменения в систему управления рисками;
- координирует деятельность Участников по обеспечению БФПС;
- осуществляет информационное взаимодействие с Участниками в целях управления рисками нарушения БФПС;
- контролирует соблюдение Участниками порядка обеспечения БФПС;
- осуществляет координацию деятельности и информационное взаимодействие Субъектов Платежной системы по обеспечению БФПС;
- определяет время, в течение которого должно быть восстановлено оказание УПИ в случае приостановления их оказания и период времени, в течение которого должно быть восстановлено оказание УПИ, соответствующее требованиям к оказанию услуг, в случае нарушения указанных требований;
- разрабатывает внутренние документы по обеспечению БФПС и управлению рисками Платежной системы и доводит необходимую информацию по управлению рисками до сведения Участников;

- контролирует внутренние документы по обеспечению БФПС и управлению рисками Операторов УПИ и Участников Платежной системы.

8.3.4.2. Операционный центр:

- уполномочен и несет ответственность за управление рисками Операционного центра;
- обеспечивает уровень бесперебойности оказания операционных услуг в стандартном режиме, установленном в п.8.3.14 Правил;
- обеспечивает снижение риска нарушения бесперебойности оказания операционных услуг путем беспрерывной круглосуточной работы программных комплексов;
- устанавливает допустимые технологические перерывы в оказании операционных услуг на основании оценки уровня рисков, общая продолжительность технологических перерывов не может превышать 48 часов в течение каждого года работы;
- собирает и обрабатывает первичную информацию о времени поступления в Платежную систему распоряжений Участников;
- предоставляет по запросу Оператора первичную информацию о функционировании Платежной системы;
- собирает и обрабатывает информацию о событиях, вызвавших операционные сбои, об их причинах и последствиях, а также в случае возникновения или реализации угрозы неисполнения, или ненадлежащего исполнения Участниками принятых на себя обязательств;
- ежемесячно (не позднее трех рабочих дней месяца, следующего за отчетным) предоставляет Оператору информацию о выявленных нарушениях БФПС за отчетный период, содержащую подробное описание характера события, вероятных причин его возникновения и последствий. В случае непредоставления данной информации, Оператор уполномочен считать, что за отчетный период у отчитывающегося оператора услуг платежной инфраструктуры отсутствуют нарушения БФПС;
- осуществляет деятельность по обеспечению бесперебойности оказания услуг Участникам в соответствии с принятыми на себя обязательствами и требованиями порядка обеспечения БФПС;
- осуществляет мониторинг рисков нарушения БФПС;
- осуществляет регулярную оценку качества и надежности функционирования применяемых информационных систем, работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Оператором и Участниками, их совершенствование;
- разрабатывает внутренние документы по обеспечению БФПС и управлению рисками в рамках выполняемых функциональных обязанностей.

8.3.4.3. Платежный клиринговый центр:

- уполномочен и несет ответственность за управление рисками Платежного клирингового центра;
- обеспечивает уровень бесперебойности оказания клиринговых услуг в стандартном режиме, установленном в п.8.3.14 Правил;
- обеспечивает снижение риска нарушения бесперебойности оказания клиринговых услуг путем беспрерывной круглосуточной работы программных комплексов;
- устанавливает допустимые технологические перерывы в оказании клиринговых услуг на основании оценки уровня рисков, общая продолжительность технологических перерывов не может превышать 48 часов в течение каждого года работы;
- осуществляет сбор и обработку информации о ходе исполнения распоряжений Участников, характеристиках осуществляемых Переводов денежных средств, количестве, сумме и

времени наступления окончательности Переводов, размере клиринговых позиций и остатках денежных средств на Счетах Участников;

- предоставляет по запросу Оператора первичную информацию о функционировании Платежной системы;
- осуществляет сбор и обработку информации о событиях, вызвавших операционные сбои, об их причинах и последствиях, а также в случае возникновения или реализации угрозы неисполнения, или ненадлежащего исполнения Участниками принятых на себя обязательств;
- ежемесячно (не позднее трех рабочих дней месяца, следующего за отчетным) предоставляет Оператору отчеты о выявленных нарушениях БФПС за отчетный период, содержащих подробное описание характера события, вероятных причин его возникновения и последствий. В случае непредоставления данной информации, Оператор уполномочен считать, что за отчетный период у отчитывающегося Оператора услуг платежной инфраструктуры отсутствуют нарушения БФПС;
- осуществляет деятельность по обеспечению бесперебойности оказания услуг Участникам в соответствии с принятыми на себя обязательствами и требованиями порядка обеспечения БФПС;
- осуществляет мониторинг рисков нарушения БФПС;
- осуществляет регулярную оценку качества и надежности функционирования применяемых информационных систем, работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Оператором и Участниками, их совершенствования;
- обеспечивает снижение риска нарушения БФПС путем исключения задержек времени окончания клирингового цикла, возникших по его вине;
- разрабатывает внутренние документы по обеспечению БФПС и управлению рисками в рамках выполняемых функциональных обязанностей.

8.3.4.4. Расчетный центр:

- уполномочен и несет ответственность за управление рисками Расчетного центра;
- обеспечивает уровень бесперебойности оказания расчетных услуг в стандартном режиме, установленном п.8.3.14 Правил;
- обеспечивает снижение риска нарушения бесперебойности оказания расчетных услуг путем беспрерывной круглосуточной работы программных комплексов;
- устанавливает допустимые технологические перерывы в оказании расчетных услуг на основании оценки уровня рисков, общая продолжительность технологических перерывов не может превышать 48 часов в течение каждого года работы;
- предоставляет по запросу Оператора первичную информацию о функционировании Платежной системы в пределах своего функционала;
- осуществляет сбор и обработку информации о событиях, вызвавших операционные сбои, об их причинах и последствиях, а также в случае возникновения или реализации угрозы неисполнения, или ненадлежащего исполнения принятых на себя обязательств;
- ежемесячно (не позднее трех рабочих дней месяца, следующего за отчетным) предоставляет Оператору отчеты о выявленных нарушениях БФПС за отчетный период, содержащих подробное описание характера события, вероятных причин его возникновения и последствий. При отсутствии выявленных нарушений БФПС за отчетный период Расчетные центры предоставляют Оператору уведомления об отсутствии выявленных нарушений БФПС за отчетный период (в свободной форме);

- осуществляет деятельность по обеспечению бесперебойности оказания услуг Участникам в соответствии с принятыми на себя обязательствами и требованиями порядка обеспечения БФПС;
- осуществляет мониторинг рисков нарушения БФПС;
- осуществляет регулярную оценку качества и надежности функционирования применяемых информационных систем, работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Оператором и Участниками, их совершенствование;
- обеспечивает снижение риска нарушения БФПС путем исключения задержек времени проведения расчетов с Участниками, возникших по его вине;
- разрабатывает внутренние документы по обеспечению БФПС и управлению рисками в рамках выполняемых функциональных обязанностей.

8.3.4.5. Участники:

- осуществляют соблюдение настоящих Правил, заключенных договоров, законодательства Российской Федерации;
- обеспечивают надлежащую защиту информации;
- обеспечивают поддержание необходимого остатка денежных средств на Счете Участника;
- разрабатывают внутренние документы по обеспечению БФПС и управлению рисками в рамках выполняемых функциональных обязанностей.

8.3.5. Субъекты Платежной системы самостоятельно организовывают и осуществляют управление рисками, присущими их виду деятельности и участия в Платежной системе. Система управления рисками каждого Субъекта Платежной системы должна включать, но не ограничиваться, назначение ответственных сотрудников и (или) наделение соответствующими полномочиями подразделений, ответственных за управление рисками и разработкой внутренних правил по управлению рисками.

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

8.3.7. Оператор проводит оценку рисков в Платежной системе «МОМЕНТОМ» с использованием методик анализа рисков в платежной системе и составлением профилей рисков согласно п.8.3.12 настоящих Правил.

8.3.8. Оператор определяет способы управления рисками в Платежной системе «МОМЕНТОМ», исходя из способов управления рисками, предусмотренных частью 5 статьи 28 Закона о НПС. Способы управления рисками определены в п.8.3.20 настоящих Правил.

8.3.9. БФПС является характеристикой Платежной системы и определяется деятельностью всех Субъектов Платежной системы, направленной на обеспечение ими как способности предупреждать нарушение требований законодательства Российской Федерации, настоящих Правил, заключенных договоров, так и восстанавливать надлежащее функционирование Платежной системы в случае его нарушения.

8.3.10. Показатели БФПС определяются в целях:

- анализа рисков нарушения БФПС;
- описания профиля рисков нарушения БФПС;
- выбора или пересмотра мер, необходимых для достижения и поддержания допустимого уровня рисков нарушения БФПС, и идентификации Субъекта Платежной системы, ответственного за их реализацию.

Для каждого устанавливаемого показателя БФПС определяется процедура и методика его формирования на основе первичной информации о функционировании Платежной системы и сведений о факторах риска нарушения БФПС.

8.3.11. Оператор Платежной системы «МОМЕНТОМ» определяет следующие показатели БФПС:

Показатель П1 - показатель продолжительности восстановления оказания УПИ, характеризующий период времени восстановления оказания услуг Операторами УПИ в случае приостановления оказания УПИ, в том числе вследствие нарушения требований к обеспечению защиты информации при осуществлении переводов денежных средств, установленных Банком России на основании части 3 статьи 27 Закона о НПС. Рассчитывается по каждому из Операторов УПИ и по каждому из Инцидентов, повлекших приостановление оказания УПИ, как период времени с момента возникновения события, приведшего к приостановлению оказания УПИ в результате первого из возникших инцидентов, и до момента восстановления оказания УПИ;

Показатель П2 - показатель непрерывности оказания УПИ, характеризующий период времени между двумя последовательно произошедшими в ПС Инцидентами, в результате которых приостанавливалось оказание УПИ. Приостановление (прекращение) участия в ПС в случаях, предусмотренных настоящими Правилами в соответствии с пунктом 4 части 1 статьи 20 Закона о НПС не рассматривается в качестве Инцидентов. Рассчитывается по каждому из Операторов УПИ при возникновении каждого из Инцидентов, повлекших приостановление оказания УПИ, как период времени между двумя последовательно произошедшими у Оператора УПИ Инцидентами, в результате которых приостанавливалось оказание УПИ, с момента восстановления оказания УПИ, приостановленных в результате первого Инцидента и до момента возникновения события, приведшего к приостановлению оказания УПИ в результате следующего Инцидента;

Показатель П3 - показатель соблюдения регламента, 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 Закона о НПС и разделом 9 настоящих Правил. Рассчитывается ежемесячно по каждому Оператору УПИ и по Платежной системе «МОМЕНТОМ» в целом. 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;

Показатель П4 - показатель доступности Операционного центра Платежной системы «МОМЕНТОМ», характеризующий оказание операционных услуг Операционным центром Платежной системы «МОМЕНТОМ». Рассчитывается ежемесячно по Операционному центру и по Платежной системе «МОМЕНТОМ» в целом. При наличии в Платежной системе нескольких операционных центров показатель П4 рассчитывается для каждого Операционного центра Платежной системы. Значение показателя П4 по Платежной системе в целом принимается равным наименьшему из значений данного показателя, рассчитанных по всем Операционным центрам Платежной системы;

Показатель П5 - показатель изменения частоты Инцидентов, характеризующий темп прироста частоты Инцидентов. Рассчитывается ежемесячно для каждого Оператора УПИ и по Платежной системе «МОМЕНТОМ» в целом.

8.3.12. Оператор проводит плановую оценку рисков в Платежной системе «МОМЕНТОМ», а также внеплановые оценки рисков в Платежной системе «МОМЕНТОМ» с использованием методик анализа рисков в Платежной системе и составлением профилей рисков.

Оператор проводит внеплановую оценку всех рисков в Платежной системе «МОМЕНТОМ» при внесении изменений в один или несколько бизнес-процессов. Проведение внеплановой оценки всех

рисков в Платежной системе «МОМЕНТОМ» завершается не позднее истечения шести месяцев со дня внесения указанных изменений.

Оператор проводит внеплановую оценку отдельных рисков (отдельного риска) в Платежной системе «МОМЕНТОМ»:

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

- при установлении по результатам проводимого Оператором мониторинга рисков факта приближения фактического (присущего) 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 «МОМЕНТОМ»;

- при выявлении значимого риска в Платежной системе «МОМЕНТОМ», для которого уровень присущего риска до применения способов управления рисками в Платежной системе «МОМЕНТОМ» может превысить или превысил уровень допустимого риска;

Проведение внеплановой оценки отдельных рисков (отдельного риска) в Платежной системе «МОМЕНТОМ» завершается не позднее истечения четырех месяцев со дня возникновения событий, предусмотренных абзацами вторым и третьим предыдущего предложения, либо со дня выявления значимого риска в Платежной системе «МОМЕНТОМ», указанного в абзаце четвертом предыдущего предложения.

Оператор проводит плановую оценку рисков в Платежной системе «МОМЕНТОМ» не реже одного раза в три года с учетом сведений о событиях, которые произошли в Платежной системе «МОМЕНТОМ» со дня завершения предыдущей плановой или внеплановой оценки всех рисков в Платежной системе и привели к приостановлению (прекращению) оказания УПИ.

Оператор устанавливает и пересматривает с использованием результатов оценки рисков в Платежной системе «МОМЕНТОМ» пороговые уровни показателей БФПС (Приложение № 3 к Правилам).

8.3.13. Оператор рассчитывает и анализирует значения показателей БФПС, в том числе путем их сравнения с пороговыми уровнями показателей БФПС (Приложение № 3 к Правилам), и использует результаты указанного анализа при оценке системы управления рисками в Платежной системе «МОМЕНТОМ» и при оценке влияния Инцидентов на БФПС.

8.3.14. В Платежной системе определены следующие режимы функционирования Платежной системы:

- стандартный – БФПС в штатном режиме, при котором ни один из показателей не превышает пороговых значений;
- приемлемый – функционирование Платежной системы с нарушениями, влияющими на БФПС, но не приводящими к нарушению функционирования Платежной системы;
- критический – функционирование Платежной системы с нарушениями, влияющими на БФПС и приводящими к невозможности оказания услуг Платежной системы.

8.3.15. Критериями надлежащего функционирования Платежной системы является соблюдение показателей БФПС и способность восстанавливать надлежащее функционирование Платежной системы в случае его нарушения.

8.3.16. Выявление факторов превышения критических значений уровня бесперебойности оказания услуг платежной инфраструктуры по одному или нескольким показателям БФПС

однозначно идентифицируется как нарушение надлежащего функционирования Платежной системы.

8.3.17. В Платежной системе устанавливаются следующие значения продолжительности периода времени, в течение которого надлежащее функционирование Платежной системы должно быть восстановлено в случае его нарушения:

- длительность восстановления надлежащего функционирования Платежной системы в случае нарушения оказания операционных услуг, в случае их приостановления (прекращения) – не более 6 часов;
- длительность восстановления надлежащего функционирования Платежной системы в случае нарушения оказания услуг платежного клиринга и расчетных услуг – не более 6 часов.

8.3.18. Система управления рисками предусматривает выполнение следующих мероприятий:

- определение организационной структуры управления рисками, обеспечивающей контроль за выполнением Участниками требований к управлению рисками, установленных настоящими Правилами;
- определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;
- доведение до Оператора соответствующей информации о рисках;
- определение показателей БФПС и других характеристик в соответствии с требованиями нормативных актов Банка России;
- определение методик анализа рисков в Платежной системе, включая профили рисков, в соответствии с требованиями нормативных актов Банка России;
- определение порядка обмена информацией, необходимой для управления рисками;
- определение 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 Платежной системе.

8.3.19. **Организационная структура системы управления рисками Оператора**

Субъекты Платежной системы внутренними документами определяют должностное лицо или структурное подразделение, к обязанностям которых относятся обеспечение мониторинга и проведение мероприятий, связанных с управлением рисками в Платежной системе. Указанные лица (структурные подразделения) подчиняются непосредственно исполнительному органу и/или единоличному исполнительному органу.

В целях управления рисками в Платежной системе, в том числе обеспечения контроля за выполнением Операторами УПИ и Участниками Платежной системы «МОМЕНТОМ» требований к управлению рисками, установленных настоящими Правилами, задействованы следующие органы и подразделения Оператора в рамках их полномочий:

- Генеральный директор;
- Служба информационной безопасности;
- Служба управления рисками;
- ИТ-подразделение;
- иные структурные подразделения и сотрудники Оператора.

Функциональные обязанности Генерального директора по управлению рисками:

- утверждение основных принципов системы управления рисками;
- утверждение внутренних документов в области управления рисками;

- рассмотрение отчетов структурных подразделений о состоянии системы управления рисками и оценке принимаемых рисков;
- принятие необходимых управленческих решений по планированию мероприятий в случае признания уровня риска высоким;
- определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
- определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;
- контроль за соблюдением всеми Участниками настоящих Правил.

Функциональные обязанности Службы информационной безопасности по управлению рисками:

- определение порядка обеспечения защиты информации в Платежной системе;
- участие в разработке внутренних документов в рамках своего функционала в области управления рисками;
- предоставление информации для расчета показателей БФПС и участие в расчете показателей БФПС и других характеристик в соответствии с требованиями нормативных актов Банка России;
- сбор информации о рисках в рамках своего функционала, в том числе информации, поступающей от Операторов УПИ и Участников.

Функциональные обязанности Службы управления рисками по управлению рисками:

- разработка внутренних документов в области управления рисками;
- определение показателей БФПС и других характеристик в соответствии с требованиями нормативных актов Банка России;
- определение методик анализа рисков в Платежной системе, включая профили рисков, в соответствии с требованиями нормативных актов Банка России;
- сбор и обработка информации о рисках, в том числе информации, поступающей от Операторов УПИ и Участников;
- мониторинг уровня рисков в Платежной системе;
- анализ и регулярная оценка уровня риска по каждому из видов рисков;
- определение допустимого уровня риска по каждому из видов рисков;
- выбор и реализация мероприятий, способов достижения и поддержания допустимого уровня рисков в Платежной системе, оценка их эффективности и совершенствования;
- установление критериев оценки системы управления рисками, включая системный риск и проведение указанной оценки;
- организация обмена информацией о рисках и мерах по управлению ими между структурными подразделениями Оператора;
- проведение оценки эффективности системы управления рисками Платежной системы «МОМЕНТОМ»;
- формирование предложений и рекомендаций по итогам проведения оценки системы управления рисками.

Функциональные обязанности ИТ по управлению рисками:

- определение порядка изменения операционных и технологических средств и процедур;
- участие в разработке внутренних документов в области управления рисками;
- выбор и реализация мероприятий, способов достижения и поддержания допустимого уровня рисков в Платежной системе, оценка их эффективности и совершенствования;
- участие в установлении критериев оценки системы управления рисками и проведении указанной оценки;

- сбор информации о рисках в рамках своего функционала, в том числе информации, поступающей от Операторов УПИ и Участников.
- мониторинг уровня рисков в Платежной системе в рамках своего функционала;
- выявление, измерение и определение допустимого уровня риска в рамках своего функционала;
- предоставление информации Службе управления рисками для расчета показателей БФПС и участие в расчете показателей БФПС и других характеристик в соответствии с требованиями нормативных актов Банка России;
- организация обмена информацией о рисках и мерах по управлению ими между структурными подразделениями Оператора.

Функциональные обязанности иных структурных подразделений и сотрудников Оператора:

- контроль за соблюдением всеми Участниками настоящих Правил в рамках своего функционала;
- сбор, обработка и доведение до Генерального директора и Службы управления рисками информации о рисках в рамках своего функционала, в том числе информации, поступающей от Операторов УПИ и Участников;
- проведение расчетов в Платежной системе в пределах, предоставленных Участниками денежных средств.

Распределение обязанностей по управлению рисками в Платежной системе между органами, подразделениями и сотрудниками Оператора устанавливается Оператором в положениях, приказах, должностных инструкциях и иных внутренних документах Оператора.

8.3.20. **Способы управления рисками**

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

В Платежной системе применяются следующие способы управления рисками:

- анализ Оператором документов Участников и Операторов услуг платежной инфраструктуры, их деловой репутации;
- управление очередностью исполнения распоряжений Участников;
- ежедневное осуществление расчетов в Платежной системе;
- проведение расчетов в Платежной системе в пределах, предоставленных Участниками денежных средств;
- создание Гарантийного фонда ПС для трансграничных переводов.

8.3.21. **Доведение до органов управления Оператора соответствующей информации о рисках**

Участники и Расчетные центры обязаны:

- незамедлительно довести до Оператора информацию о рисках в случае наступления чрезвычайных ситуаций или значительного нарушения допустимого уровня риска (включая случаи системных сбоев) в виде письменных отчетов, в том числе в электронном виде по согласованным каналам связи;
- информировать обо всех выявленных Инцидентах в виде отчета по форме № 0403205 «Сведения по инцидентам, возникшим (выявленным) при оказании услуг платежной инфраструктуры, и показателям бесперебойности функционирования платежной системы» ежемесячно не позднее десятого рабочего дня месяца, следующего за отчетным (при отсутствии инцидентов Участники и Расчетные центры предоставляют в адрес Оператора уведомления, подтверждающие отсутствие инцидентов в отчетном периоде в свободной форме).

Консолидированная информация обо всех выявленных рисках доводится до сведения органов управления Оператора не реже одного раза в квартал Руководителем Службы управления рисками в виде отчетов в разрезе каждого из рисков. При отсутствии информации о выявленных рисках формируются и предоставляются в адрес Оператора уведомления, подтверждающие данную информацию.

Информирование об общем уровне рисков в Платежной системе происходит не реже одного раза в год в виде письменных отчетов Руководителя Службы управления рисками Генеральному директору Оператора.

8.3.22. Оператор проводит оценку системы управления рисками в Платежной системе «МОМЕНТОМ», в том числе используемых методов оценки рисков в Платежной системе, результатов применения способов управления рисками в Платежной системе «МОМЕНТОМ», не реже одного раза в три года и документально оформляет результаты указанной оценки.

8.3.23. 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 УПИ в течение периодов времени, установленных Оператором в настоящих Правилах, при их приостановлении. Оператор при управлении рисками в Платежной системе «МОМЕНТОМ» оценивает риски, возникающие в связи с привлечением поставщиков (провайдеров), предоставляющих услуги в сфере информационных технологий в целях оказания оператором УПИ услуг платежной инфраструктуры и (или) предоставляющих услуги обмена информацией при осуществлении операций с использованием электронных средств платежа между операторами по переводу денежных средств и иностранными поставщиками платежных услуг, предусмотренные пунктом 33 статьи 3 Закона о НПС (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.

8.3.24. 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.

8.3.25. Оператор определяет профили рисков (Приложение № 6 к настоящим Правилам) 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.

8.3.26. В качестве экспертов выступают специалисты Оператора, привлеченные специалисты Субъектов Платежной системы, также могут привлекаться внешние эксперты.

8.4. Управление непрерывностью функционирования Платежной системы

8.4.1. Оператор организует деятельность по управлению непрерывностью функционирования Платежной системы «МОМЕНТОМ», в том числе путем установления прав и обязанностей Субъектов Платежной системы по управлению непрерывностью функционирования Платежной системы в зависимости от организационной модели управления рисками в Платежной системе, определенной в соответствии с требованиями части 2 статьи 28 Закона о НПС.

В качестве организационной модели управления рисками в Платежной системе принята модель, предусматривающая распределение функций по оценке и управлению рисками между Оператором, Операторами услуг платежной инфраструктуры и Участниками.

8.4.2. Права, обязанности и функции Субъектов Платежной системы, в том числе и по управлению непрерывностью функционирования Платежной системы, в зависимости от

организационной модели управления рисками в Платежной системе рассмотрены в п.8.3.4 настоящих Правил.

8.4.3. Оператор организует сбор и обработку сведений, в том числе от привлеченных Операторов УПИ, используемых для расчета показателей БФПС, указанных в п.8.3.11 настоящих Правил.

8.4.4. Операторы услуг платежной инфраструктуры предоставляют следующую информацию об Инциденте:

	Время и дата возникновения и/или выявления (нужное подчеркнуть) Инцидента (формат время ХХ:ХХ:ХХ дата ХХ.ХХ.ХХ)
Краткое описание Инцидента, характеристика произошедшего события, его последствия	
Наименование одного или нескольких бизнес-процессов, в ходе которого(ых) произошел Инцидент	
Наименование одного или нескольких бизнес-процессов, на который(е) оказал влияние Инцидент	
Наличие/отсутствие факта приостановления/прекращения оказания УПИ в результате Инцидента	
Влияние Инцидента на БФПС	
Степень влияния Инцидента на функционирование ПС «МОМЕНТОМ» в зависимости от количества операторов УПИ, и/или количества и значимости участников ПС «МОМЕНТОМ», на которых оказал непосредственное влияние Инцидент, и/или количества и суммы неисполненных, и/или ошибочно исполненных распоряжений Участников ПС «МОМЕНТОМ», и иных факторов (информация, которой располагает Оператор УПИ)	

Время и дата восстановления оказания УПИ в случае приостановления их оказания	
Мероприятия по устранению неблагоприятных последствий Инцидента с указанием планируемой и фактической продолжительности проведения данных мероприятий	
Дата восстановления оказания УПИ, соответствующего требованиям к оказанию услуг	
Неблагоприятные последствия Инцидента по Субъектам ПС «МОМЕНТОМ», в том числе: - сумма денежных средств, уплаченных Оператором ПС «МОМЕНТОМ» и/или взысканных с него - сумма денежных средств, уплаченных оператором(ми) УПИ и/или взысканных с него(них) - количество и сумма неисполненных, и/или несвоевременно исполненных, и/или ошибочно исполненных распоряжений Участников ПС «МОМЕНТОМ», на исполнение которых оказал влияние Инцидент - продолжительность приостановления оказания УПИ	

8.4.5. Оператор обеспечивает хранение сведений по Платежной системе и сведений об Инцидентах не менее пяти лет с даты получения указанных сведений.

8.4.6. Оператор организует деятельность по разработке регламентов выполнения процедур и контролирует их наличие и соблюдение.

8.4.7. Оператор проводит оценку влияния на БФПС каждого произошедшего в Платежной системе «МОМЕНТОМ» Инцидента в срок не позднее окончания рабочего дня, следующего за днем возникновения (выявления) Инцидента, а также в срок не позднее окончания рабочего дня следующего за днем устранения последствий Инцидента (восстановления оказания УПИ, соответствующих требованиям к оказанию услуг).

8.4.8. Оператор классифицирует Инциденты, произошедшие в ПС «МОМЕНТОМ», как непосредственно не влияющие на БФПС и влияющие на БФПС.

8.4.9. Оператор проводит оценку влияния на БФПС всех Инцидентов, произошедших в Платежной системе в течение календарного месяца. Оценка влияния на БФПС данных Инцидентов проводится в течение пяти рабочих дней после дня окончания календарного месяца, в котором возникли Инциденты.

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

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

8.4.11. Оператор определяет следующие критерии отнесения событий, реализовавшихся при оказании УПИ в Платежной системе «МОМЕНТОМ» к событиям приостановления оказания УПИ – непредоставление услуг УПИ более 2 часов, за исключением событий, следствием которых является приостановление оказания УПИ в связи с проведением технологических и (или) регламентных работ (плановых и внеплановых), в случае если Оператор УПИ уведомил Оператора и Участников заранее, не позднее одного рабочего дня до даты начала проведения работ, в том числе работ, вызванных необходимостью устранения чрезвычайных обстоятельств, повлиявших на работоспособность Платежной системы. В уведомлении Оператор УПИ указывает предполагаемые дату и время начала и окончания проведения указанных работ и направляет его по согласованным каналам связи Оператору и Участникам Платежной системы «МОМЕНТОМ» в соответствии с настоящими Правилами и (или) иными документами Оператора и (или) привлеченных Операторов УПИ.

Оператор определяет следующий период времени, в течение которого должно быть восстановлено оказание УПИ в случае приостановления их оказания – 6 часов, и период времени, в течение которого должно быть восстановлено оказание УПИ, соответствующее требованиям к оказанию услуг – 6 часов, в случае нарушения указанных требований.

8.4.12. 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.

8.4.13. Оператор устанавливает следующие уровни оказания УПИ, характеризующие качество функционирования операционных и технологических средств платежной инфраструктуры, которые должны быть обеспечены Операторами УПИ:

- оказание УПИ, соответствующих требованиям к оказанию услуг;
- оказание УПИ, не соответствующих требованиям к оказанию услуг.

Качество функционирования операционных и технологических средств платежной инфраструктуры, которое должно быть обеспечено Операторами УПИ, оценивается Оператором ежемесячно вместе с определением показателей БФПС.

К УПИ, соответствующих требованиям к оказанию услуг, относятся УПИ при которых одновременно соблюдаются:

- требования законодательства Российской Федерации, настоящие Правила Платежной системы «МОМЕНТОМ», заключенные договоры при взаимодействии Субъектов Платежной системы;

- временной регламент функционирования Платежной системы, определенный в разделе 9 настоящих Правил;
- пороговые уровни показателей БФПС, определенные в Приложении № 3 к настоящим Правилам;
- время восстановления оказания УПИ в случае приостановления, прекращения их оказания и время восстановления оказания УПИ, соответствующих требованиям к оказанию УПИ, в случае нарушения указанных требований, определенные в настоящих Правилах - 6 часов.

Оказанием УПИ, несоответствующих требованиям к оказанию услуг, считаются УПИ, оказываемые Операторами УПИ, при которых не соблюдаются все или одно из указанных выше условий.

8.4.14. Оператор разрабатывает, тестирует и пересматривает план действий, направленный на обеспечение непрерывности деятельности и (или) восстановление деятельности в случае возникновения нестандартных и чрезвычайных ситуаций (далее - план ОНиВД) Оператора Платежной системы, с периодичностью не реже одного раза в два года.

8.4.15. 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, порядок взаимодействия в спорных, нестандартных и чрезвычайных ситуациях (включая случаи системных сбоев), в том числе:

- при совмещении в Платежной системе функций Оператора и Операционного, и (или) Платежного клирингового, и (или) Расчетного центров – мероприятия по переходу на резервный комплекс программных и (или) технологических средств, а также мероприятия, осуществляемые в случае неработоспособности систем и сервисов поставщиков услуг, нарушение предоставления которых способно привести к приостановлению оказания УПИ;
- при наличии в Платежной системе двух и более Операционных, и (или) Платежных клиринговых, и (или) Расчетных центров - мероприятия по обеспечению взаимозаменяемости Операторов УПИ;
- при наличии в Платежной системе одного привлеченного Операционного, и (или) Платежного клирингового, и (или) Расчетного центров - мероприятия по привлечению другого Оператора УПИ и по переходу Участников Платежной системы на обслуживание к вновь привлеченному Оператору УПИ в течение 20 (двадцать) рабочих дней, в случаях:
    - превышения Оператором УПИ времени восстановления оказания УПИ при приостановлении их оказания более двух раз в течение трех месяцев подряд,
    - нарушения Правил, выразившегося в отказе Оператора УПИ в одностороннем порядке от оказания услуг Участнику (Участникам) Платежной системы, не связанного с приостановлением (прекращением) участия в Платежной системе в случаях, предусмотренных настоящими Правилами.

8.4.16. Оператор обеспечивает реализацию мероприятий, предусмотренных п.8.4.15 настоящих Правил.

8.4.17. Субъекты Платежной системы обязаны осуществлять разработку, проверку (тестирование) и пересмотр плана ОНиВД по мере необходимости, но не реже 1 (одного) раза в 2 (два) года. План ОНиВД в соответствии с требованиями федерального законодательства и нормативно-правовых актов Банка России и иных контролирующих органов должен определять порядок, способы и сроки осуществления комплекса мероприятий по предотвращению или своевременной ликвидации последствий возможного нарушения режима функционирования Субъекта Платежной системы, вызванного непредвиденными обстоятельствами (возникновением чрезвычайной ситуации или иным событием, наступление которого возможно, но трудно

предсказуемо и связано с угрозой существенных материальных потерь или иных последствий, препятствующих выполнению Субъектом Платежной системы принятых на себя обязательств).

В случае если Субъект Платежной системы является кредитной организацией, то разработка, проверка (тестирование) и пересмотр плана ОНиВД должны осуществляться в том числе согласно порядку, предусмотренному Положением Банка России от 16.12.2003 № 242-П «Об организации внутреннего контроля в кредитных организациях и банковских группах», с учетом требований к плану ОНиВД, содержащихся в п.8.4.15 настоящих Правил.

8.4.18. Оператор организует разработку (при необходимости) и контролирует наличие планов ОНиВД у Операторов УПИ, проведение ими проверки (тестирования) и пересмотра планов ОНиВД с периодичностью не реже 1 (одного) раза в 2 (два) года.

В целях контроля за выполнением указанной обязанности Оператор с периодичностью не реже 1 (Одного) раза в 2 (два) года направляет в адрес Оператора УПИ запрос о предоставлении копии плана ОНиВД и информации о проведении проверки (тестирования) и пересмотра плана ОНиВД. По результатам анализа указанных документов Оператор, в случае выявления недочетов и наличия замечаний, направляет в адрес Оператора УПИ рекомендации по устранению выявленных недочетов.

8.4.19. Оператор анализирует эффективность мероприятий по восстановлению оказания УПИ, соответствующего требованиям к оказанию услуг, и использует полученные результаты при управлении рисками в Платежной системе.

8.5. Организация взаимодействия Субъектов Платежной системы по обеспечению БФПС

8.5.1. Оператор определяет порядок взаимодействия Субъектов Платежной системы при реализации мероприятий, предусмотренных п.8.3 и п.8.4 настоящих Правил.

8.5.2. Оператор организует деятельность по организации взаимодействия Субъектов Платежной системы «МОМЕНТОМ», в том числе путем установления прав и обязанностей Субъектов Платежной системы, в зависимости от организационной модели управления рисками в Платежной системе, определенной в соответствии с требованиями части 2 статьи 28 Закона о НПС.

В качестве организационной модели управления рисками в Платежной системе принята модель, предусматривающая распределение функций по оценке и управлению рисками между Оператором, Операторами услуг платежной инфраструктуры и Участниками.

8.5.3. Права, обязанности и функции Субъектов Платежной системы, в том числе и по порядку взаимодействия, в зависимости от организационной модели управления рисками в Платежной системе рассмотрены в п.8.3.4 настоящих Правил.

8.5.4. Оператор определяет функции, выполняемые Операторами УПИ по оперативному информированию Оператора Платежной системы о нарушении оказания УПИ, соответствующего требованиям к оказанию услуг, при котором превышено время восстановления оказания УПИ в случае их приостановления и (или) время восстановления оказания УПИ, соответствующего требованиям к оказанию услуг.

8.5.5. Оператор информирует о случаях и причинах приостановления (прекращения) оказания УПИ:

- Банк России и Участников Платежной системы в порядке, установленном Указанием Банка России от 11 июня 2014 года № 3280-У «О порядке информирования оператором платежной системы Банка России, участников платежной системы о случаях и причинах приостановления (прекращения) оказания услуг платежной инфраструктуры» (далее - Указание Банка России № 3280-У);
- операторов УПИ в порядке, аналогичном установленному Указанием Банка России № 3280-У для Участников Платежной системы.

8.6. Контроль за соблюдением Операторами УПИ и Участниками Платежной системы порядка обеспечения БФПС

8.6.1. Оператор в рамках осуществления контроля за соблюдением Правил проверяет соблюдение Операторами УПИ и Участниками Платежной системы порядка обеспечения БФПС с учетом следующих требований.

8.6.1.1. Оператор определяет следующий порядок проведения контроля за соблюдением Операторами УПИ и Участниками Платежной системы порядка обеспечения БФПС:

- контроль предоставления первичной информации о функционировании Платежной системы по запросу Оператора;
- контроль ежемесячного предоставления Оператору информации о выявленных нарушениях БФПС за отчетный период, содержащих подробное описание характера события, вероятных причин его возникновения и последствий (в случае непредоставления данной информации Оператор уполномочен считать, что за отчетный период у отчитывающегося Оператора УПИ отсутствуют нарушения БФПС);
- контроль наличия и актуальности разработанных Операторами УПИ внутренних документов по обеспечению БФПС и управлению рисками в рамках выполняемых функциональных обязанностей;
- расчет показателей БФПС и контроль соблюдения пороговых уровней показателей БФПС, определенных в Приложении № 3 к настоящим Правилам;
- контроль соблюдения временного регламента функционирования Платежной системы, определенного в разделе 9 настоящих Правил.

8.6.1.2. Операторам УПИ необходимо разработать и поддерживать в актуальном состоянии следующие документы по обеспечению БФПС Платежной системы в рамках своего функционала:

- Положение о порядке обеспечения бесперебойности функционирования Платежной системы «МОМЕНТОМ»;
- План ОНиВД.

8.6.1.3. Оператор контролирует соответствие документов, разработанных Операторами УПИ согласно настоящего пункта и п.п. 8.3.4.2 - 8.3.4.4 настоящих Правил, порядку обеспечения БФПС, и, при выявлении несоответствия документов Операторов УПИ порядку обеспечения БФПС, направляет рекомендации Операторам УПИ по устранению выявленных несоответствий.

8.6.1.4. Оператор при выявлении нарушения порядка обеспечения БФПС Операторами УПИ и Участниками Платежной системы:

- информирует Операторов УПИ и Участников Платежной системы о выявленных в их деятельности нарушениях и устанавливает сроки устранения нарушений;
- осуществляет проверку результатов устранения нарушений и информирует Операторов УПИ и Участников Платежной системы, в деятельности которых выявлены нарушения, о результатах проведенной проверки.

8.6.1.5. Оператор определяет ответственность за несоблюдение порядка обеспечения БФПС. Порядок обеспечения БФПС определен в настоящих Правилах. Ответственность за несоблюдение настоящих Правил, в том числе ответственность Операторов УПИ и Участников Платежной системы за неисполнение порядка обеспечения БФПС, определена в п.2.2 настоящих Правил.

8.7. Методики анализа рисков в Платежной системе, включая профили рисков

8.7.1. Оператор в целях управления рисками в Платежной системе разрабатывает методики анализа рисков в Платежной системе, включая риск нарушения БФПС. Анализ рисков осуществляется с использованием не менее чем одного метода из числа предусмотренных таблицей А.2 приложения А к Стандарту. Основными используемыми методами являются метод синдинического подхода (принимающего во внимание цели, ценности, настоящие Правила Платежной системы

«МОМЕНТОМ», данные причастных сторон, выявляющего противоречия, упущения и формирующего источники и факторы риска), метод индексов риска (оценивающего значимость рисков), а также элементы метода экспертных оценок.

Оператор устанавливает следующую классификацию и дает определение рисков.

Правовой риск – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие несоблюдения Субъектами ПС требований законодательства Российской Федерации, Правил Платежной системы «МОМЕНТОМ», договоров, заключенных между Субъектами ПС, документов Оператора и документов Операторов УПИ либо вследствие наличия правовых коллизий и (или) правовой неопределенности в законодательстве Российской Федерации, нормативных актах Банка России, Правилах Платежной системы «МОМЕНТОМ» и договорах, заключенных между Субъектами ПС, а также вследствие нахождения Операторов УПИ и Участников ПС под юрисдикцией различных государств.

Операционный риск – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие возникновения у Субъектов ПС 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 ПС либо вследствие воздействия событий, причины возникновения которых не связаны с деятельностью Субъектов, включая чрезвычайные ситуации, ошибочные или противоправные действия третьих лиц.

Кредитный риск – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, центральным платежным клиринговым контрагентом или расчетным центром ПС вследствие невыполнения Участниками ПС договорных обязательств перед указанными организациями в установленный срок или в будущем.

Риск ликвидности – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие отсутствия у центрального платежного клирингового контрагента и (или) у Участников ПС денежных средств, достаточных для своевременного выполнения их обязательств перед другими Субъектами ПС.

Общий коммерческий риск – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие ухудшения финансового состояния Оператора и/или Операторов УПИ, не связанного с реализацией кредитного риска ПС и риска ликвидности ПС.

Системный риск – это риск оказания УПИ, не соответствующего требованиям к оказанию услуг, вследствие неспособности одного или нескольких Субъектов ПС исполнить принятые на себя обязательства или нарушений в самой ПС, вследствие которой большинство или все Субъекты ПС не способны исполнить свои обязательства в срок. Возникновение системного риска является следствием возникновения двух или более рисков, указанных выше.

8.7.2. Методики анализа рисков в Платежной системе обеспечивают:

- выполнение процедур выявления Оператором рисков в Платежной системе «МОМЕНТОМ» не реже одного раза в год;
- проведение анализа рисков в Платежной системе;
- выявление событий, реализация которых может привести к возникновению Инцидента (далее - риск-события), и определение для каждого из выявленных риск-событий уровня риска, характеризуемого вероятностью наступления риск-событий и величиной возможных последствий их реализации (далее - уровень риска);
- определение для каждого из выявленных рисков в Платежной системе уровня присущего риска до применения способов управления рисками в Платежной системе (далее - уровень присущего риска), а также уровня допустимого риска, указанного в абзаце третьем четвертого предложения подпункта 8.3.12 настоящих Правил; определение

значимых рисков в Платежной системе, указанных в абзаце четвертом четвертого предложения подпункта 8.3.12 настоящих Правил;

- определение для каждого из значимых рисков в Платежной системе, указанных в абзаце четвертом четвертого предложения подпункта 8.3.12 настоящих Правил, уровня остаточного риска после применения способов управления рисками в Платежной системе (далее - уровень остаточного риска).

8.7.3. Методики анализа рисков в Платежной системе предусматривают выполнение следующих мероприятий:

- формирование и поддержание в актуальном состоянии перечней бизнес-процессов (Приложение № 5 к настоящим Правилам);
- разработку и поддержание в актуальном состоянии классификаторов (структурированных перечней) рисков в Платежной системе, риск-событий, причин риск-событий;
- проведение анализа бизнес-процессов в Платежной системе, в том числе анализа программных и (или) технических средств Операторов УПИ, учитывая факт привлечения ими поставщиков услуг, и других факторов, влияющих на БФПС;
- формирование перечня возможных риск-событий для каждого бизнес-процесса с указанием причин риск-событий и их последствий;
- 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 абзаце третьем четвертого предложения подпункта 8.3.12 настоящих Правил;
- сопоставление уровня присущего риска до применения способов управления рисками в Платежной системе и уровня допустимого риска, указанного в абзаце третьем четвертого предложения подпункта 8.3.12 настоящих Правил, по каждому из выявленных рисков в Платежной системе для определения значимых рисков в Платежной системе, указанных в абзаце четвертом четвертого предложения подпункта 8.3.12 настоящих Правил;
- применение способов управления рисками в Платежной системе для каждого из значимых рисков в Платежной системе, указанных в абзаце четвертом четвертого предложения подпункта 8.3.12 настоящих Правил, и последующее определение для них уровня остаточного риска после применения способов управления рисками в Платежной системе;
- сопоставление уровня остаточного риска после применения способов управления рисками в Платежной системе и уровня допустимого риска, указанного в абзаце третьем четвертого предложения подпункта 8.3.12 настоящих Правил, для каждого из значимых рисков в Платежной системе, указанных в абзаце четвертом четвертого предложения подпункта 8.3.12 настоящих Правил, и принятие решения о необходимости применения других способов управления рисками в Платежной системе в дополнение к ранее примененным способам;
- мониторинг рисков в Платежной системе, в том числе уровня остаточного риска после применения способов управления рисками в Платежной системе, его соответствия уровню допустимого риска, указанного в абзаце третьем четвертого предложения подпункта 8.3.12 настоящих Правил,;
- составление и пересмотр (актуализацию) профиля каждого из значимых рисков в Платежной системе, указанных в абзаце четвертом четвертого предложения подпункта 8.3.12 настоящих Правил, включая профиль риска нарушения БФПС (Приложение № 6 к настоящим Правилам) (далее - профили рисков).

8.7.4. Оператор составляет профили рисков по всем значимым рискам в Платежной системе, указанным в абзаце четвертом четвертого предложения подпункта 8.3.12 настоящих Правил, в том числе по рискам, указанным в подпункте 8.7.1 настоящих Правил.

Оператор составляет профили рисков в соответствии с требованиями, предусмотренными в нормативных документах Банка России, и пересматривает (актуализирует) их по результатам плановой или внеплановой оценки всех рисков в Платежной системе, а также внеплановой оценки отдельных рисков (отдельного риска) в Платежной системе.

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

8.8. Порядок изменения операционных и технологических средств и процедур

8.8.1. Решение о необходимости изменения операционных и технологических средств и процедур принимает Оператор.

8.8.2. Основанием для изменения операционных и технологических средств и процедур являются:

- включение новых типов операций по Переводам денежных средств или внесение существенных изменении в действующие операции;
- замена или модернизация операционных и технологических средств, направленных на повышение качества оказания услуг по Переводу денежных средств;
- внесение изменений в функционирование системы управления рисками;
- изменение действующего законодательства Российской Федерации.

8.8.3. Если изменение операционных и технологических средств и процедур требует внесения изменений в настоящие Правила, Оператор вносит соответствующие изменения в порядке, предусмотренном для внесения изменений в Правила.

8.8.4. Если изменение операционных и технологических средств и процедур не требует внесения изменений в настоящие Правила, Оператор направляет Участникам соответствующее уведомление с описанием изменений не позднее, чем за тридцать календарных дней до даты вступления в силу соответствующих изменений.

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

8.9.1. Оператор осуществляет оценку качества функционирования информационных систем, операционных и технологических средств и процедур Платежной системы самостоятельно или с привлечением независимой организации.

8.9.2. Для самостоятельной оценки качества функционирования информационных систем, операционных и технологических средств Оператор осуществляет сбор первичной информации от Операторов услуг платежной инфраструктуры:

- информации о возникших в процессе работы информационных систем, операционных и технологических средств, нарушениях и неисправностях;
- результатов проведения самооценки уровня БФПС и уровня риска нарушения БФПС;
- сравнение расчетных значений уровня риска с принятыми в Платежной системе;
- анализ динамики изменения уровня риска;
- в случае превышения допустимого уровня риска или негативной динамики уровня риска, принятие решения о модернизации или замене используемых информационных систем, операционных и технологических средств.

8.9.3. Оценка качества функционирования информационных систем, операционных и технологических средств с привлечением независимой организации включает в себя следующие мероприятия, осуществляемые Оператором:

- принятие решения о привлечении независимой организации;

- выбор сторонней организации;
- заключение договора со сторонней организацией;
- предоставление сторонней организации информации, необходимой для проведения оценки;
- выполнение сторонней независимой организацией работ по оценке качества и надёжности функционирования информационных систем, операционных и технологических средств;
- получение от сторонней организации отчёта с результатами оценки и с рекомендациями по совершенствованию информационных систем, операционных и технологических средств.

8.9.4. На основании результатов оценки качества функционирования операционных и технологических средств и информационных систем Платежной системы независимой организацией и рекомендаций по совершенствованию Оператор вносит изменения в функционирование операционных и технологических средств и процедур Платежной системы в порядке, предусмотренном для внесения изменений в Правила.

9. Временной регламент функционирования Платежной системы

9.1. Операционный день

9.1.1. Платежная система функционирует в режиме 24/7/365 (24 часа, 7 дней в неделю, 365 дней в году).

9.1.2. В Платежной системе устанавливается операционный день с 00:00:00 МСК до 23:59:59 МСК календарного дня.

9.2. Временной регламент

9.2.1. В качестве единой шкалы времени при расчетах в Платежной системе признается московское время. Контрольным является время системных часов аппаратных средств Оператора. Время проведения расчетов представлено в Таблице №1, регламенты обработки распоряжений и проведения расчетов представлены в Таблице №2.

9.2.2. Платежный клиринг осуществляется в отношении Участников, не менее 2 (двух) раз в день по рабочим дням, в соответствии с Временным регламентом (Таблица № 2).

Таблица 1.

Время приёма к исполнению распоряжений Отправителей и Участников

Событие	Время по Московскому времени
Прием распоряжений Отправителей	Круглосуточно
Прием распоряжений Участников	Круглосуточно

Таблица 2.

Регламент обработки распоряжений и проведения расчетов Отправителей и Участников.

Регламентные работы	Временной интервал	Исполнитель
День 1		
Прием и передача распоряжений Участников к обработке в ПКЦ	С 00:00:00 до 23:59:59	Операционный центр
Прием к исполнению, формирование и отправка принятых и обработанных распоряжений Участников.	С 00:00:00 до 23:00:00	Платежный клиринговый центр

Формирование платежно-клиринговой позиции Участников		
Передача Реестра нетто позиций Участникам и Расчетному центру	С 00:00:00 до 23:00:00	Платежный клиринговый центр
Проведение расчетов и информирование Платежного клирингового центра о проведении расчетов между Участниками	С 23:00:01 до 23:59:59	Расчетный центр
День 2		
Передача Прямым Участникам распоряжений с отметкой об исполнении в соответствии с условиями договора Счета Прямого Участника	с 00:00:00 до 11:00:00	Расчетный центр

Расчёты проводятся ежедневно, по рабочим дням. Дата проведения расчетов по Счетам Прямых Участников соответствует дате проведения платежной операции Клиентов, либо в случае выходных/праздничных дней переносится на первый рабочий день.

9.2.3. О проведении плановых технических, профилактических и ремонтных работ Оператор уведомляет Участников заблаговременно, не позднее, чем за пять рабочих дней до даты начала проведения работ, путем опубликования на Сайте Платежной системы. В уведомлении указываются дата и время начала проведения работ, предполагаемые дата и время окончания проведения работ.

9.2.4. О проведении внеплановых ремонтных работ, а также работ, вызванных необходимостью устранения чрезвычайных обстоятельств, повлиявших на работоспособность Платежной системы, Оператор уведомляет Участников не позднее одного рабочего дня с даты начала проведения работ, путем опубликования на Сайте Платежной системы. В уведомлении указываются предполагаемые дата и время окончания проведения работ.

9.2.5. Внесение изменений во временной регламент функционирования Платежной системы осуществляется в общем порядке, предусмотренном для внесения изменений в Правила.

9.3. Расчеты с использованием конвертации

9.3.1. Оператор предоставляет Участникам возможность осуществлять Услуги с использованием конвертации, в том числе при условии соблюдении требований национального законодательства страны нахождения Прямого Участника/Партнера.

9.3.2. Курс конвертации устанавливается Расчетным центром или Оператором. Актуальная информация о курсе конвертации (его смене) размещается Расчетным центром/Оператором в ПС, и является справочной для ознакомления Клиентами/Участниками перед оказанием Услуг.

9.3.3. РЦ/Оператор вправе в любое время в одностороннем порядке изменять курс конвертации.

9.3.4. ПС «МОМЕНТОМ» осуществляет конвертацию по курсу, установленному на момент оказания Услуг.

9.3.5. Финансовые обязательства Участника, обслуживающего Отправителя, перед Оператором ПС при осуществлении списания Перевода денежных средств с конвертацией возникают в Валюте приема распоряжения на Перевод денежных средств.

9.3.6. Финансовые обязательства Оператора ПС перед Участником, обслуживающим Получателя, при осуществлении зачисления Перевода денежных средств с конвертацией возникают в Валюте зачисления распоряжения на Перевод денежных средств.

9.3.7. Расчет платежной клиринговой позиции при осуществлении операций с конвертацией осуществляется в той валюте, в которой возникают обязательства Участника или Оператора.

9.3.8. При возврате или аннулировании Перевода денежных средств, осуществленного с конвертацией, сумма распоряжения Перевода денежных средств и комиссии за него (в случае ее возврата) возвращается Оператором ПС Участнику, обслуживающему Отправителя, - в Валюте приема распоряжения на Перевод денежных средств, по курсу, установленному на момент отправки Перевода.

10.Обеспечение защиты информации в Платежной системе

10.1. Общие положения о защите информации в Платежной системе

10.1.1. Правила устанавливают общие требования к защите информации, обрабатываемой Субъектами Платежной системы, подлежащей обязательной защите в соответствии с законодательством Российской Федерации, а также защите в соответствии:

- требованиями законодательства в области защиты информации;
- нормативными актами Банка России;
- требованиями к защите информации, установленными Правительством Российской Федерации, включая Постановление Правительства Российской Федерации от 13 июня 2012 года №584 «Об утверждении Положения о защите информации в платежной системе»;
- Настоящими Правилами.

10.1.2. Защита информации обеспечивается путем реализации Субъектами Платежной системы правовых, организационных и технических мер, направленных:

- на соблюдение конфиденциальности информации;
- на реализацию права на доступ к информации в соответствии с законодательством Российской Федерации;
- на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий в отношении информации.

10.1.3. Субъекты Платежной системы утверждают внутренние документы, устанавливающие порядок реализации требований к защите информации, не противоречащие настоящим Правилам.

10.1.4. Для проведения работ по защите информации и контроля (оценки) соблюдения требований к защите информации Субъектами Платежной системы могут привлекаться на договорной основе организации, имеющие лицензии на деятельность по технической защите конфиденциальной информации и (или) на деятельность по разработке и производству средств защиты конфиденциальной информации.

10.1.5. Оператор, Участники, Расчетный центр обязаны пересматривать действующий порядок обеспечения защиты информации при осуществлении Переводов денежных средств в связи с изменениями требований к защите информации, определенных законодательными актами Российской Федерации, нормативными актами Правительства Российской Федерации и Банка России, Правилами, изменениями установленных в Правилах требований к защите информации, выявлением недостатков при осуществлении контроля выполнения порядка обеспечения защиты информации, в сроки, указанные в нормативных документах.

10.1.6. Требования к защите информации не применяются, в случаях отсутствия обработки, включая прием, передачу и хранение защищаемой информации, в том числе в случаях отсутствия переводов денежных средств в рамках ПС.

10.2. Информация, подлежащая защите при осуществлении Переводов денежных средств

10.2.1. Требования к обеспечению защиты информации, установленные настоящими Правилами, при осуществлении Переводов денежных средств применяются для обеспечения защиты следующей информации:

- информации о совершенных Переводах денежных средств, в том числе информации, содержащейся в извещениях (подтверждениях), касающихся приема к исполнению распоряжений Участников, а также в извещениях (подтверждениях), касающихся исполнения распоряжений Участников;
- информации об остатках денежных средств на банковских счетах;
- информации, содержащейся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях Клиентов по Переводу денежных средств, распоряжениях Участников, распоряжениях Платежного клирингового центра;
- информации о платежных клиринговых позициях;
- информации, необходимой для удостоверения Клиентами права распоряжения денежными средствами;
- информации о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования, эксплуатация которых обеспечивается Участником, Оператором услуг платежной инфраструктуры и используемых для осуществления Переводов денежных средств, а также информации о конфигурации, определяющей параметры работы технических средств по защите информации;
- ключевой информации средств криптографической защиты информации (далее СКЗИ), используемых при осуществлении Переводов денежных средств (далее – криптографические ключи);
- 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.

10.3. Требования к обеспечению защиты информации в Платежной системе

10.3.1. Требования к обеспечению защиты информации при осуществлении Переводов денежных средств включают в себя:

10.3.1.1. Требования к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемые для защиты информации на стадиях создания, эксплуатации (использования по назначению, технического обслуживания и ремонта), модернизации, снятия с эксплуатации Объектов информационной инфраструктуры;

10.3.1.2. 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;

10.3.1.3. 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);

10.3.1.4. Требования к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемые для защиты информации при использовании Интернет при осуществлении Переводов денежных средств;

10.3.1.5. Требования к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемые для защиты информации при использовании Интернет при осуществлении Переводов денежных средств;

10.3.1.6. Требования к обеспечению защиты информации при осуществлении переводов денежных средств, применяемые для защиты информации при использовании СКЗИ;

10.3.1.7. 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);

10.3.1.8. Требования к организации и функционированию подразделения (работников), ответственного (ответственных) за организацию и контроль обеспечения защиты информации в лице службы ИБ и (или) ответственного за ИБ в организации;

10.3.1.9. Требования к повышению осведомленности работников Участника, являющегося юридическим лицом, Оператора услуг платежной инфраструктуры и Клиентов (далее - повышение осведомленности) в области обеспечения защиты информации;

10.3.1.10. Требования к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, и реагированию на них;

10.3.1.11. Требования к определению и реализации порядка обеспечения защиты информации при осуществлении Переводов денежных средств;

10.3.1.12. Требования к оценке выполнения Оператором, Участником, Оператором услуг платежной инфраструктуры требований к обеспечению защиты информации при осуществлении Переводов денежных средств;

10.3.1.13. Требования к доведению Участником, ОУПИ до Оператора информации об обеспечении в ПС защиты информации при осуществлении Переводов денежных средств;

10.3.1.14. Требования к совершенствованию Оператором, Участником, ОУПИ защиты информации при осуществлении Переводов денежных средств;

10.3.1.15. Требования по противодействию осуществлению Переводов денежных средств без согласия Клиента

10.4. Способы выполнения требований к обеспечению защиты информации при осуществлении Переводов денежных средств

10.4.1. Выполнение требований к обеспечению защиты информации при осуществлении Переводов денежных средств обеспечивается путем:

10.4.1.1. Выбора организационных мер защиты информации; определения во внутренних документах Оператора, Участника, ОУПИ 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;

10.4.1.2. Выбора технических средств защиты информации; определения во внутренних документах Оператора, Участника, ОУПИ 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.

10.5. Состав требований к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемых для защиты информации на стадиях создания, эксплуатации, модернизации, снятия с эксплуатации объектов информационной инфраструктуры

10.5.1. В состав требований к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемых для защиты информации на стадиях создания, эксплуатации, модернизации, снятия с эксплуатации объектов информационной инфраструктуры, включаются следующие требования:

10.5.1.1. Оператор, Участник, ОУПИ обеспечивают включение в технические задания на создание (модернизацию) объектов информационной инфраструктуры требований к обеспечению защиты информации при осуществлении Переводов денежных средств.

10.5.1.2. Оператор, Участник, ОУПИ обеспечивают участие службы ИБ и (или) ответственного за ИБ в разработке и согласовании технических заданий на создание (модернизацию) объектов информационной инфраструктуры.

10.5.1.3. Оператор, Участник, ОУПИ обеспечивают контроль со стороны службы ИБ и (или) ответственного за ИБ соответствия создаваемых (модернизируемых) объектов информационной инфраструктуры требованиям технических заданий.

10.5.1.4. Помимо этого, Оператор, Участник, ОУПИ обеспечивают:

- наличие эксплуатационной документации на используемые технические средства защиты информации;
- контроль выполнения требований эксплуатационной документации на используемые технические средства защиты информации в течение всего срока их эксплуатации;
- восстановление функционирования технических средств защиты информации, используемых при осуществлении Переводов денежных средств, в случаях сбоев и (или) отказов в их работе.

10.5.1.5. Оператор, Участник, ОУПИ обеспечивают реализацию запрета использования защищаемой информации на стадии создания объектов информационной инфраструктуры.

10.5.1.6. Оператор, Участник, ОУПИ на стадиях эксплуатации и снятия с эксплуатации объектов информационной инфраструктуры обеспечивают:

- реализацию запрета несанкционированного копирования защищаемой информации;
- защиту резервных копий защищаемой информации;
- уничтожение защищаемой информации в случаях, когда указанная информация больше не используется, за исключением защищаемой информации, перемещенной в архивы, ведение и сохранность которых предусмотрены законодательными актами Российской Федерации, нормативными актами Банка России, Правилами и (или) договорами, заключенными Участником, Оператором, ОУПИ;

Оператор, Участник, ОУПИ обеспечивают уничтожение защищаемой информации, в том числе содержащейся в архивах, способом, обеспечивающим невозможность ее восстановления.

10.6. Состав требований к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемых для защиты информации при осуществлении доступа к объектам информационной инфраструктуры

10.6.1. 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:

10.6.1.1. Участник, ОУПИ обеспечивают учет объектов информационной инфраструктуры, используемых для обработки, хранения и (или) передачи защищаемой информации;

10.6.1.2. Участник, ОУПИ обеспечивают применение некриптографических средств защиты информации от несанкционированного доступа, в том числе прошедших в установленном порядке процедуру оценки соответствия.

10.6.1.3. При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных выше, Участник, ОУПИ обеспечивают:

- выполнение процедур идентификации, аутентификации, авторизации своих работников при осуществлении доступа к защищаемой информации;
- идентификацию, аутентификацию, авторизацию Участников при осуществлении Переводов денежных средств;
- определение порядка использования информации, необходимой для выполнения аутентификации;
- регистрацию действий при осуществлении доступа своих работников к защищаемой информации;
- регистрацию действий, связанных с назначением и распределением прав доступа к защищаемой информации.

10.6.1.4. При осуществлении доступа к защищаемой информации, находящейся на объектах информационной инфраструктуры, указанных выше, Участник, ОУПИ 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.

10.6.1.5. 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.

10.6.1.6. Участник, ОУПИ обеспечивают:

- реализацию запрета несанкционированного расширения прав доступа к защищаемой информации;
- назначение своим работникам минимально необходимых для выполнения их функциональных обязанностей прав доступа к защищаемой информации.

10.6.1.7. Участник, ОУПИ 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, 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, ОУПИ и которые используются для осуществления Переводов денежных средств (далее - средства вычислительной техники), и телекоммуникационное оборудование, эксплуатация которого обеспечивается Участником, ОУПИ 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.

10.6.1.8. В случае принятия Участником, ОУПИ решения о необходимости применения организационных мер защиты информации и (или) использования технических средств защиты информации, указанных выше, Участник, ОУПИ обеспечивают применение указанных организационных мер защиты информации и (или) использование указанных технических средств защиты информации.

10.6.1.9. Участник, ОУПИ обеспечивают принятие мер, направленных на предотвращение хищений носителей защищаемой информации.

Участник обеспечивает возможность приостановления (блокирования) Клиентом приема к исполнению распоряжений об осуществлении Переводов денежных средств от имени указанного Клиента.

10.7. Состав требований к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемых для защиты информации от воздействия вредоносного кода

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

10.7.1.1. Участник, ОУПИ обеспечивают:

- использование технических средств защиты информации, предназначенных для выявления вредоносного кода и для предотвращения воздействия вредоносного кода на объекты информационной инфраструктуры (далее - технические средства защиты информации от воздействия вредоносного кода), на средствах вычислительной техники, платежных терминалах и иных общедоступных объектах доступа, в случае их использования в рамках ПС и при наличии технической возможности;
- регулярное обновление версий технических средств защиты информации от воздействия вредоносного кода и баз данных, используемых в работе технических средств защиты информации от воздействия вредоносного кода и содержащих описание вредоносных кодов и способы их обезвреживания;
- функционирование технических средств защиты информации от воздействия вредоносного кода в автоматическом режиме, при наличии технической возможности.

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

10.7.3. Участник, ОУПИ обеспечивают использование технических средств защиты информации от воздействия вредоносного кода различных производителей и их раздельную установку на персональных электронных вычислительных машинах и серверах, используемых для осуществления Переводов денежных средств, а также на межсетевых экранах, задействованных в осуществлении Переводов денежных средств, при наличии технической возможности.

10.7.4. При наличии технической возможности Участник, ОУПИ обеспечивают выполнение:

- предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, в случае их использования в рамках ПС;
- проверки на отсутствие вредоносного кода средств вычислительной техники, в случае их использования в рамках ПС.

10.7.5. В случае обнаружения вредоносного кода или факта воздействия вредоносного кода Участник, Оператор, ОУПИ обеспечивают принятие мер, направленных на предотвращение распространения вредоносного кода и устранение последствий воздействия вредоносного кода.

10.8. Состав требований к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемых для защиты информации при использовании сети Интернет при осуществлении Переводов денежных средств

10.8.1. 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:

10.8.1.1. При использовании сети Интернет для осуществления Переводов денежных средств Участник, ОУПИ:

- применение организационных мер защиты информации и (или) использование технических средств защиты информации, предназначенных для предотвращения доступа к содержанию защищаемой информации, передаваемой по сети Интернет;
- 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;
- 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;
- 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;
- фильтрацию сетевых пакетов при обмене информацией между вычислительными сетями, в которых располагаются объекты информационной инфраструктуры, и сетью Интернет.

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

10.9. Защита информации при осуществлении Переводов денежных средств с использованием СКЗИ

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

10.9.2. Защита информации при осуществлении Переводов денежных средств с использованием СКЗИ осуществляется в следующем порядке:

10.9.2.1. Работы по обеспечению защиты информации с помощью СКЗИ проводятся в соответствии с Федеральным законом от 6 апреля 2011 года N 63-ФЗ «Об электронной подписи» (Собрание законодательства Российской Федерации, 2011, N 15, ст. 2036; N 27, ст. 3880), Положением о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005), утвержденным приказом ФСБ России от 9 февраля 2005 года N 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 N 24), и технической документацией на СКЗИ.

10.9.2.2. В случае если Участник, ОУПИ применяют СКЗИ российского производителя, указанные СКЗИ должны иметь сертификаты уполномоченного государственного органа.

10.9.2.3. Участник и ОУПИ могут не применять СКЗИ в случаях, установленных законодательством Российской Федерации, в том числе Банком России и ФСБ России и (или) в случаях неактуальности угроз, связанных с нарушением конфиденциальности и целостности

информации при их передачи по Интернет или иным недоверенным сетям, с учетом результатов моделирования угроз и (или) оценки рисков информационной безопасности.

10.9.2.4. В случае применения СКЗИ Участник, ОУПИ обязан применять СКЗИ, которые:

- допускают встраивание СКЗИ в технологические процессы осуществления Переводов денежных средств, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;
- поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;
- поддерживают непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований.

10.9.2.5. В случае применения СКЗИ Участник, ОУПИ определяют во внутренних документах и выполняют порядок применения СКЗИ, включающий:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в автоматизированные системы, используемые для осуществления Переводов денежных средств;
- порядок эксплуатации СКЗИ;
- 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;
- порядок снятия с эксплуатации СКЗИ;
- порядок управления ключевой системой;
- порядок обращения с носителями криптографических ключей, включая порядок применения организационных мер защиты информации и использования технических средств защиты информации, предназначенных для предотвращения несанкционированного использования криптографических ключей, и порядок действий при смене и компрометации ключей.

10.9.2.6. При применении СКЗИ криптографические ключи могут изготавливаться Клиентом самостоятельно, либо изготавливаться Оператором, ОУПИ и (или) Участником. 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.

10.10. Состав требований к обеспечению защиты информации при осуществлении Переводов денежных средств, применяемых для защиты информации с использованием технологических мер защиты информации

10.10.1. 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:

10.10.1.1. Участник, ОУПИ обеспечивают учет и контроль состава, установленного и (или) используемого на средствах вычислительной техники программного обеспечения;

10.10.1.2. 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 ОУПИ обеспечивают выполнение указанного порядка.

10.10.1.3. При эксплуатации объектов информационной инфраструктуры Участник, ОУПИ обеспечивают:

- защиту электронных сообщений от искажения, фальсификации, переадресации, несанкционированного ознакомления и (или) уничтожения, ложной авторизации;
- контроль (мониторинг) соблюдения установленной технологии подготовки, обработки, передачи и хранения электронных сообщений и защищаемой информации на объектах информационной инфраструктуры;
- аутентификацию входных электронных сообщений;
- взаимную (двустороннюю) аутентификацию участников обмена электронными сообщениями; восстановление информации об остатках денежных средств на банковских счетах или выхода из строя средств вычислительной техники;
- сверку выходных электронных сообщений с соответствующими входными и обработанными электронными сообщениями при осуществлении расчетов в Платежной Системе; выявление фальсифицированных электронных сообщений, в том числе осуществление операций, связанных с осуществлением Переводов денежных средств, злоумышленником от имени авторизованного Клиента (подмена авторизованного клиента) после выполнения процедуры авторизации.

10.11. Состав требований к организации и функционированию службы ИБ

10.11.1. В состав требований к организации и функционированию службы ИБ включаются следующие требования:

10.11.1.1. Участник, ОУПИ:

- обеспечивают формирование Службы ИБ и (или) назначение ответственного за ИБ, а также определяют во внутренних документах цели и задачи деятельности этой службы;
- предоставляют полномочия и выделяют ресурсы, необходимые для выполнения Службой ИБ и (или) ответственным за ИБ установленных целей и задач.

10.11.1.2. Участник, ОУПИ назначают куратора службы ИБ и (или) ответственного за ИБ из состава своего органа управления и определяют его полномочия. При этом служба ИБ (ответственный за ИБ) и служба ИТ (ответственный за ИТ) не должны иметь общего куратора, а сам куратор должен быть подотчетен органу управления в целом и (или) его руководителю (главе).

10.11.1.3. Служба ИБ и (или) ответственный за ИБ осуществляет планирование и контроль обеспечения защиты информации при осуществлении Переводов денежных средств, для чего наделяется следующими полномочиями:

- осуществлять контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении Переводов денежных средств;
- определять требования к техническим средствам защиты информации и организационным мерам защиты информации;
- контролировать выполнение работниками требований к обеспечению защиты информации при осуществлении Переводов денежных средств;
- участвовать в разбирательствах инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, и предлагать применение дисциплинарных взысканий, а также направлять предложения по совершенствованию защиты информации;
- 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.

10.12. Состав требований к повышению осведомленности в области обеспечения защиты информации

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

10.12.1.1. Участник, ОУПИ обеспечивают повышение осведомленности работников в области обеспечения защиты информации:

- по порядку применения организационных мер защиты информации;
- по порядку использования технических средств защиты информации.

10.12.1.2. Участник, ОУПИ обеспечивают повышение осведомленности работников, получивших новую роль, связанную с применением организационных мер защиты информации или использованием технических средств защиты информации.

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

10.13. Состав требований к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, и реагирования на них

10.13.1. В состав требований к выявлению инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, и реагирования на них включаются следующие положения и требования:

10.13.1.1. Оператор определяет:

- требования к порядку, форме и срокам информирования Оператора, Участников и ОУПИ о выявленных в Платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств; информирование Оператора о выявленных Участниками и ОУПИ, привлекаемыми для оказания Услуг платежной инфраструктуры в Платежной системе инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, осуществляется ежемесячно;
- требования к взаимодействию Оператора, Участников и ОУПИ в случае выявления в инциденты, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств.

10.13.1.2. Участник, ОУПИ обеспечивают выполнение указанных в настоящем подпункте требований.

10.13.1.3. Участник, ОУПИ обеспечивают:

- применение 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;
- информирование службы ИБ и (или) ответственного за ИБ, о выявлении инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств;
- реагирование на выявленные инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств;
- анализ причин выявленных инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, проведение оценки результатов реагирования на такие инциденты.

10.13.1.4. Оператор обеспечивает учет и доступность для Участников и ОУПИ, привлекаемых для оказания Услуг платежной инфраструктуры в ПС, информации:

- о выявленных в ПС инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств;
- о выявленных в ПС инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств;
- о методиках анализа и реагирования на инциденты, связанные с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств.

10.13.2. Оператор устанавливает следующий порядок взаимодействия субъектов ПС 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:

10.13.2.1. В случае выявления инцидента, связанного с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств в Платежной системе, ОУПИ, Участники должны незамедлительно, но не позднее одного часа с момента выявления инцидента, сообщить о нём в доступной форме по Согласованным каналам связи и по форме установленной Оператором (Приложение № 4 к Правилам). При необходимости оперативного информирования допускается обращение по другим каналам связи в вольном формате, с последующим дублированием сообщения согласно описанному выше порядку.

10.13.2.2. Служба ИБ и (или) ответственный за ИБ Оператора, инициирует информирование Участников и ОУПИ в доступной форме по Согласованным каналам связи 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 ОУПИ.

10.13.3. Оператор устанавливает следующее содержанию, форму и периодичность предоставления информации, направляемой ОУПИ и Участниками Оператору для целей анализа обеспечения в Платежной системе защиты информации при осуществлении Переводов денежных средств:

10.13.3.1. Для целей анализа обеспечения в Платежной системе защиты информации при осуществлении Переводов денежных средств, Участники и ОУПИ направляют в Службу ИБ и (или) ответственному за ИБ Оператора посредством Согласованных каналов связи на ежеквартальной основе не позднее пятнадцатого рабочего дня месяца, следующего за отчетным кварталом, в электронном виде отчет о выявленных инцидентах по форме 0403203, предусмотренной Указанием Банка России от 27 июня 2023 г. N 6470-У «О формах, методиках составления, порядке и сроках представления отчетности оператора платежной системы, оператора услуг платежной инфраструктуры, оператора по переводу денежных средств в Центральный банк Российской Федерации». При этом, такой отчет предоставляется Оператору исключительно в отношении инцидентов, выявленных при работе в Платежной системе.

10.13.3.2. 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.

10.13.4. Оператор устанавливает следующий Порядок обеспечения учета и доступности для Участников и ОУПИ информации о выявленных в ПС инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств в ПС, и методиках анализа и реагирования на инциденты:

10.13.4.1. Служба ИБ и (или) ответственный за ИБ Оператора ведет учет выявленных в Платежной системе инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, в соответствии с внутренними процедурами, разработанными Оператором;

10.13.4.2. 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 ОУПИ в форме отчета на ежемесячной основе. В случае отсутствия инцидентов за отчетный период, такой отчет отправляется незаполненным. Кроме того, соответствующая информация предоставляется Участникам и ОУПИ по их письменному запросу.

10.13.4.3. 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.

10.13.4.4. 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 ОУПИ 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.

10.14. Состав требований к определению и реализации порядка обеспечения защиты информации при осуществлении Переводов денежных средств

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

10.14.1.1. Документы, составляющие порядок обеспечения защиты информации при осуществлении Переводов денежных средств, определяют:

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

10.14.1.2. Оператор устанавливает распределение обязанностей по определению порядка обеспечения защиты информации при осуществлении Переводов денежных средств путем:

- их фиксации в настоящих Правилах;
- самостоятельного определения Оператором порядка обеспечения защиты информации при осуществлении переводов денежных средств в иных документах Оператора;
- распределения обязанностей по определению порядка обеспечения защиты информации при осуществлении переводов денежных средств между Оператором, ОУПИ и Участниками, в том числе на основании заключаемых между сторонами договоров;

10.14.1.3. Оператор, Участник, ОУПИ обеспечивают определение порядка обеспечения защиты информации при осуществлении Переводов денежных средств в рамках распределения обязанностей, установленных Оператором Платежной системы.

10.14.1.4. Для определения порядка обеспечения защиты информации при осуществлении Переводов денежных средств Оператор, Участник, ОУПИ в рамках обязанностей, установленных Оператором, могут использовать:

- положения национальных стандартов по защите информации, стандартов организаций, в том числе стандартов Банка России, рекомендаций в области стандартизации, в том числе рекомендаций Банка России, принятых в соответствии с законодательством Российской Федерации о техническом регулировании;
- положения документов, определяемых международными платежными системами;
- 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, ОУПИ;
- иные источники, не противоречащие требования Российского законодательства.

10.14.1.5. Участник, ОУПИ обеспечивают выполнение порядка обеспечения защиты информации при осуществлении Переводов денежных средств.

10.14.1.6. Участник, ОУПИ обеспечивают назначение лиц, ответственных за выполнение порядка обеспечения защиты информации при осуществлении Переводов денежных средств.

10.14.1.7. Служба ИБ и (или) ответственный за информационную безопасность Участника, ОУПИ осуществляет контроль (мониторинг) выполнения порядка обеспечения защиты информации при осуществлении Переводов денежных средств, включая:

- контроль (мониторинг) применения организационных мер защиты информации;

контроль (мониторинг) использования технических средств защиты информации.

10.15. Состав требований к оценке выполнения Оператором, Участником, ОУПИ требований к обеспечению защиты информации при осуществлении Переводов денежных средств

10.15.1. Участник, Оператор, ОУПИ обеспечивают проведение оценки выполнения требований к обеспечению защиты информации при осуществлении Переводов денежных средств (далее - оценка соответствия).

10.15.2. Оценка соответствия осуществляется на основе:

10.15.2.1. Информации на бумажном носителе и (или) в электронном виде, содержащей подтверждения выполнения порядка применения организационных мер защиты информации и использования технических средств защиты информации;

10.15.2.2. Анализа соответствия порядка применения организационных мер защиты информации и использования технических средств защиты информации требованиям законодательства Российской Федерации;

10.15.2.3. Результатов контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств.

10.15.3. Оценка соответствия осуществляется Участником, Оператором, ОУПИ самостоятельно или с привлечением сторонних организаций, имеющих право на проведение соответствующих работ, в том числе лицензии ФСТЭК России на техническую защиту конфиденциальной информации, согласно определенным Банком России требованиям.

10.15.4. Оператор, Участник, ОУПИ обеспечивают проведения оценки соответствия с периодичностью и согласно порядку, определенному в соответствии с законодательством Российской федерации и нормативно-правовым актам Банка России, но не реже одного раза в два года, с использованием методологии ГОСТ Р 57580.2-2018.

10.15.5. Отчет о проведении оценки соответствия предоставляется Оператору по переводу денежных средств в соответствии с формой отчетности № 0403202, предусмотренной Указанием Банка России от 27 июня 2023 г. N 6470-У «О формах, методиках составления, порядке и сроках представления отчетности оператора платежной системы, оператора услуг платежной инфраструктуры, оператора по переводу денежных средств в Центральный банк Российской Федерации».

10.16. Состав требований к доведению Участником, ОУПИ до Оператора информации об обеспечении в Платежной системе защиты информации при осуществлении переводов денежных средств

10.16.1. В состав требований к доведению Участником, ОУПИ до Оператора информации об обеспечении в Платежной системе защиты информации при осуществлении Переводов денежных средств включаются следующие требования:

10.16.1.1. Оператор устанавливает требования к содержанию, форме и периодичности представления информации, направляемой Участниками и ОУПИ Оператору для целей анализа обеспечения в Платежной системе защиты информации при осуществлении Переводов денежных средств.

10.16.1.2. Участник и ОУПИ обеспечивают выполнение указанных требований.

10.16.1.3. Информация, направляемая Участниками и ОУПИ, Оператору для целей анализа обеспечения в ПС защиты информации при осуществлении Переводов денежных средств, включает следующую информацию:

- степени выполнения требований к обеспечению защиты информации при осуществлении Переводов денежных средств;
- реализации порядка обеспечения защиты информации при осуществлении Переводов денежных средств;
- выявленных инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств;
- результатах проведенных оценок соответствия;
- выявленных угрозах и уязвимостях в обеспечении защиты информации.

10.17. Состав требований к совершенствованию Оператором, Участником, ОУПИ защиты информации при осуществлении Переводов денежных средств

10.17.1. В состав требований к совершенствованию Оператором, Участником, ОУПИ защиты информации при осуществлении Переводов денежных средств включаются следующие требования:

10.17.1.1. Оператор, Участник, ОУПИ регламентируют пересмотр порядка обеспечения защиты информации при осуществлении Переводов денежных средств в рамках обязанностей, установленных Оператором, в связи:

- с изменениями требований к защите информации, определенных настоящими Правилами;
- с изменениями, внесенными в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе;
- с полученным опытом, в том числе связанным с возникновением новых угроз, рисков и уязвимостей защиты информации при осуществлении Переводов денежных средств, а также по результатам выявленных недостатков работы ПС.

10.17.1.2. Участник, ОУПИ регламентируют порядок принятия мер, направленных на совершенствование защиты информации при осуществлении Переводов денежных средств, в случаях:

- изменения требований к защите информации, определенных Правилами;
- изменений, внесенных в законодательные акты Российской Федерации, нормативные акты Банка России, регулирующие отношения в национальной платежной системе;

- изменения порядка обеспечения защиты информации при осуществлении Переводов денежных средств;
- выявления угроз, рисков и уязвимостей в обеспечении защиты информации при осуществлении Переводов денежных средств;
- выявления недостатков при осуществлении контроля (мониторинга) выполнения порядка обеспечения защиты информации при осуществлении переводов денежных средств;
- выявления недостатков при проведении оценки соответствия.

10.17.1.3. Принятие решений по совершенствованию защиты информации при осуществлении Переводов денежных средств согласуется с собственной Службой ИБ и (или) ответственным за ИБ.

10.17.1.4. Принятие решений по совершенствованию защиты информации при осуществлении Переводов денежных средств согласуется с собственной Службой ИБ и (или) ответственным за ИБ.

В инициативном порядке передовой опыт по совершенствованию защиты информации может транслироваться Участником и ОУПИ по Согласованным каналам связи Оператору для принятия решений об его адаптации и (или) распространению на ПС, в том числе путем изменения настоящих Правил и (или) иных документов Оператора.

10.18. Состав требований по противодействию осуществлению Переводов денежных средств без согласия клиента

10.18.1. Участник обеспечивает реализацию мероприятий по выявлению и противодействию осуществлению переводов денежных средств без согласия клиента, в соответствии с законодательством Российской Федерации и нормативными актами Банка России, в том числе, обладающих признаками осуществления перевода денежных средств без согласия клиента, устанавливаемых Банком России.

10.18.2. Участник при выявлении переводов денежных средств (попыток), осуществляемых без согласия клиента, направляет уведомление в соответствующие службы Банка России в срок, установленный Банком России, а также информирует о таких событиях Службу ИБ и (или) ответственного за ИБ Оператора в течение 24 часов после выявления соответствующего события по Согласованным каналам связи.

10.18.3. В целях реализации мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента Участник должен:

10.18.3.1. Выявлять операции по переводу денежных средств, соответствующие признакам осуществления перевода денежных средств без согласия клиента.

10.18.3.2. Выявлять операции по переводу денежных средств, совершенные в результате несанкционированного доступа к объектам информационной инфраструктуры Участника.

10.18.3.3. Выявлять компьютерные атаки, направленные на объекты информационной инфраструктуры Участника, которые могут привести к случаям и (или) попыткам осуществления переводов денежных средств без согласия клиента.

10.18.3.4. Осуществлять сбор технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Участника.

10.18.3.5. Осуществлять сбор сведений об обращении клиента в правоохранительные органы при их наличии.

10.18.3.6. Расследовать случаи и (или) попытки осуществления переводов денежных средств без согласия клиента, вызванные компьютерными атаками, направленными на объекты информационной инфраструктуры Участника.

10.18.3.7. Реализовывать меры по выявлению и устранению причин и последствий компьютерных атак, направленных на объекты информационной инфраструктуры Участника, и дальнейшему предотвращению случаев и (или) попыток осуществления переводов денежных средств без согласия клиента.

10.18.3.8. 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 Участника операций (осуществляемой клиентами деятельности) в соответствии с частью 5.1 статьи 8 Федерального закона N 161-ФЗ.

10.18.3.9. Использовать выявленную Участником информацию о технических данных, описывающих компьютерные атаки, направленные на объекты информационной инфраструктуры Участника, в целях противодействия осуществлению переводов денежных средств без согласия клиента.

11.Обеспечение защиты персональных данных в Платежной системе

11.1. Субъекты Платежной системы обеспечивают в своей деятельности соблюдение требований законодательства Российской Федерации о работе с персональными данными и несут предусмотренную законодательством Российской Федерации ответственность за несоблюдение указанных требований.

11.2. Участники, если предусмотрено законодательством Российской Федерации, информируют и в случае необходимости получают согласие лиц на обработку их персональных данных и предоставление их персональных данных Субъектам Платежной системы.

12.Информационное взаимодействие при выявлении Инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств

12.1. Субъект Платежной системы при выявлении в Платежной системе Инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, принимает меры по снижению негативных последствий, вызванных нарушением требований, информирует Субъекта Платежной системы, в функциональной зоне ответственности которого находится область возникновения Инцидента. Субъект Платежной системы, допустивший Инцидент, реализует комплекс мер, направленных на устранение причин, вызвавших Инцидент, на недопущение его повторного возникновения и последствий Инцидента. Субъект Платежной системы при выявлении в Платежной системе Инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, обязан незамедлительно информировать Оператора о выявленных Инцидентах, а также обязан незамедлительно проинформировать Оператора при выявлении в Платежной системе Инцидентов, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств по электронной почте на адрес info@momentom.su.

12.2. Оператор информирует Операторов услуг платежной инфраструктуры и Участников о выявленных в Платежной системе Инцидентах, связанных с нарушениями требований к обеспечению защиты информации при осуществлении Переводов денежных средств, носящих системный характер, а также о рекомендуемых методиках анализа и реагирования на указанные Инциденты путем размещения соответствующей информации в Личном кабинете Участника Платежной системы.

12.3. Участники и Расчетный центр предоставляют Оператору данные о выявленных ими в Платежной системе инцидентах по нарушению требований обеспечения информационной безопасности. Информирование производится в течение 10 (Десяти) рабочих дней со дня выявления инцидента, путем направления специального уведомления по форме Приложения № 4 к настоящим Правилам.

Субъекты Платежной системы по запросу Оператора предоставляют данные для целей анализа обеспечения в Платежной системе защиты информации при осуществлении Переводов денежных средств, по форме Приложения № 4 к настоящим Правилам.

12.4. Участники и Расчетный центр по запросу Оператора не позднее десяти рабочих дней предоставляют информацию о реализации порядка обеспечения и степени выполнения требований защиты информации при осуществлении Переводов денежных средств в соответствии со своими функциями в Платежной системе. Оператор имеет право потребовать предоставить копии всех документов, составляющих порядок обеспечения защиты информации при осуществлении Переводов денежных средств или выборочно по применению организационных мер защиты информации, по порядку использования технических средств защиты информации или по порядку регистрации и хранения информации на бумажных носителях и (или) в электронном виде.

12.5. Указанные сведения предоставляются Участниками и Операторами услуг платежной инфраструктуры в электронном виде на адрес ответственного лица Оператора.

13.Обеспечение банковской и коммерческой тайны в Платежной системе

13.1. Субъекты Платежной системы гарантируют в своей деятельности соблюдение банковской тайны в отношении информации, ставшей известной Субъекту Платежной системы в связи с выполнением возложенных на него функций в соответствии с Правилами.

13.2. Субъекты Платежной системы гарантируют в своей деятельности соблюдение коммерческой тайны в отношении информации, ставшей известной Субъекту Платежной системы в связи с выполнением возложенных на него функций в соответствии с Правилами.

14.Взаимодействие с другими Платежными системами

14.1. Платежная система не осуществляет взаимодействие с другими платежными системами. В случае возникновения необходимости такого взаимодействия, Оператор определяет в Правилах порядок взаимодействия и создает перечень платежных систем, с которыми осуществляется взаимодействие.

15.Порядок досудебного разрешения споров с Участниками и Операторами услуг платежной инфраструктуры

15.1. В случае возникновения между Субъектами Платежной системы споров и разногласий, возникающих из настоящих Правил или в связи с ними, стороны таких споров и разногласий будут принимать все меры к их разрешению путем переговоров.

15.2. В случае невозможности разрешения указанных споров и разногласий путем переговоров Субъекты Платежной системы, являющиеся сторонами спора и разногласия, обязуются соблюдать установленный настоящими Правилами претензионный порядок урегулирования споров и разногласий.

15.3. Претензия заявляется в письменной форме и должна быть подписана уполномоченным представителем лица, заявляющего претензию.

Претензия должна содержать:

- изложение требований заявителя;
- указание суммы претензии и её расчет (если претензия подлежит денежной оценке);
- изложение обстоятельств, являющихся основанием для требований заявителя и доказательства со ссылкой на соответствующие нормы законодательства Российской Федерации;
- перечень прилагаемых к претензии документов и других доказательств, иные сведения, необходимые для урегулирования спора.

Претензия вручается под расписку или направляется заказным письмом с уведомлением о вручении.

15.4. Претензия должна быть рассмотрена в течение трех рабочих дней со дня её получения. Если к претензии не приложены документы, необходимые для её рассмотрения, они запрашиваются у заявителя претензии. При этом указывается срок, необходимый для их представления. В случае неполучения затребованных документов к указанному сроку претензия рассматривается на основании имеющихся документов в течение трех рабочих дней с даты получения запрошенных документов, либо с даты окончания срока их представления. В любом случае общий срок рассмотрения претензии не может превышать тридцать календарных дней.

15.5. Ответ на претензию должен быть составлен в письменной форме и подписан уполномоченным представителем стороны, отвечающей за претензию. Ответ на претензию передается под расписку уполномоченному представителю её заявителя, либо направляется в адрес заявителя посредством услуг почтовой связи заказным письмом с уведомлением о вручении.

15.6. Все споры и разногласия между Субъектами Платежной системы, возникающие из настоящих Правил или в связи с ними, в случае неурегулирования их в досудебном порядке подлежат разрешению в Арбитражном суде г.Москвы.

16.Документы, составляющие Правила

16.1. Правила Платежной системы «МОМЕНТОМ»;

16.2. Приложение № 1 «Заявление на участие в Платежной системе «МОМЕНТОМ»

16.3. Приложение № 2 «Тарифы и порядок оплаты услуг по Переводу денежных средств и услуг платежной инфраструктуры»

16.4. Приложение № 3 «Пороговые уровни показателей БФПС Платежной системы «МОМЕНТОМ»;

16.5. Приложение № 4 «Форма для оперативного информирования Оператора Платежной системы о выявленных инцидентах информационной безопасности»;

16.6. Приложение № 5 «Бизнес-процессы Платежной системы «МОМЕНТОМ»;

16.7. Приложение № 6 «Профиль риска»;

16.8. Приложение № 7 «Сведения о переводах в результате НСД к объектам его инфраструктуры».

Приложение № 1
к Правилам Платежной системы «МОМЕНТОМ»

ООО «РСМП»

от: _____
_____
Адрес: _____
_____

ЗАЯВЛЕНИЕ
на участие в Платежной системе «МОМЕНТОМ»

Дата:

Настоящим _____ *(наименование организации)* в лице _____ *(Ф.И.О. и должность уполномоченного представителя Заявителя)*, действующего (-ей) на основании_____ *(наименование документа, уполномочивающего представителя Заявителя на подачу данного заявления от имени Заявителя)* (далее – «Заявитель»),

направляет Оператору Платежной системы «МОМЕНТОМ» ООО «РСМП» (далее – «Оператор») данное заявление со следующим статусом участия:

☐ Прямое участие

☐ Косвенное участие*

* В случае подачи заявления на косвенное Участие в ПС «МОМЕНТОМ» - необходимо указать через какого Прямого Участника будут осуществляться платежный клиринг и расчеты:

Полное наименование Прямого Участника, номер банковской лицензии	**Адрес местонахождения Прямого Участника:**

1. В целях рассмотрения Оператором настоящего заявления и принятия решения о возможности участия Заявителя в Платежной системе «МОМЕНТОМ» Заявитель направляет в адрес Оператора документы согласно перечню, указанному в пункте 7 настоящего Заявления. Заявитель подтверждает полноту и достоверность данных, содержащихся в прилагаемых документах.

2. Оригиналы документов предоставляются за подписью уполномоченного лица Заявителя и должны содержать оттиск печати Заявителя.

3. Заявитель подтверждает, что ознакомился с Правилами Платежной системы «МОМЕНТОМ», размещенными на Сайте Платежной системы, действующими на дату настоящего заявления, и заявляет о своем согласии с указанными Правилами.

4. Заявитель понимает и соглашается с тем, что факт получения Оператором настоящего Заявления не влечет автоматического присоединения Заявителя к Платежной системе.

5. По всем вопросам, связанным с настоящим заявлением, просим обращаться к нашему ответственному сотруднику _____ (ФИО и должность ответственного сотрудника) по телефону_____ или адресу электронной почты _____.

6. Настоящее заявление составлено в 1 (одном) экземпляре на _____ листах.

7. Перечень прилагаемых документов для Участников-резидентов:

1. Нотариально заверенные копии лицензий на осуществление операций в рублях и иностранной валюте;
2. Нотариально заверенные копии учредительных документов:
   * Устав и все изменения и дополнения к нему с приложением свидетельств об их государственной регистрации (для акционерных обществ и обществ с ограниченной или дополнительной ответственностью);
   * Учредительный договор.
3. Нотариально заверенная копия Свидетельства о государственной регистрации юридического лица (форма № Р51001) или Свидетельства о внесении записи в Единый государственный реестр юридических лиц о юридическом лице, зарегистрированном до 1 июля 2002 года (форма № Р57001).
4. Нотариально заверенная карточка с образцами подписей и, если предусмотрено, оттиском печати.
5. Выписка из протокола/решения о создании, заверенная подписью Руководителя и печатью или нотариально.
6. Выписка из протокола/решения об избрании Руководителя (единоличного исполнительного органа), заверенная подписью Руководителя и печатью или нотариально.
7. Нотариально заверенные копии писем о подтверждении согласования на должность лиц, указанных в карточке образцов подписей с территориальным учреждением Банка России (для кредитных организаций).
8. Распорядительные акты (приказы) о назначении на должность лиц, указанных в Карточке с образцами подписей и, если предусмотрено, оттиском печати. (копии)
9. Документы (доверенности/приказы), подтверждающие предоставление права подписи лицам, указанным в Карточке с образцами подписей. (копии)
10. Доверенность, подтверждающая полномочия лица, подписавшего Договор участия, если Договор участия подписывает не Руководитель. (копия)
11. Анкета Участника по переводу денежных средств, подписанная уполномоченным лицом и скрепленная печатью (предоставляется по форме Заявителя). В случае изменений анкетных данных, Участник предоставляет новую Анкету.
12. Письмо об осуществлении мер по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма (для кредитных организаций) подписанное уполномоченным лицом и скрепленное печатью.

Перечень документов для Участника-нерезидента аналогичен п.7 настоящего Заявления, с поправкой на требования национального законодательства страны такого Участника.

От имени Заявителя

_____ (должность)
_____ (Ф.И.О.)
_____ (подпись)
М.П.

«СОГЛАСОВАНО»
От имени Прямого Участника

_____ (должность)
_____ (Ф.И.О.)
_____ (подпись)
М.П.

Приложение № 2
к Правилам Платежной системы «МОМЕНТОМ»

Тарифы и порядок
оплаты услуг по Переводу денежных средств и услуг платежной инфраструктуры

1. Общие положения

1.1. Оператор имеет право вносить изменения в Тарифы Платежной системы. При внесении изменений, предусматривающих введение новых Тарифов или увеличение размера Тарифов, Оператор обязан уведомить об этом Банк России в срок не менее чем за 30 календарных дней до дня введения в действие изменений с предоставлением обоснований указанных изменений.

1.2. Оператор имеет право в пределах тарифной сетки, заявленной в Тарифах Платежной системы, в одностороннем порядке менять размер комиссии, уплачиваемой Оператором Участникам за обслуживание Клиентов. При этом информацию об изменениях размера комиссий, причитающихся Участникам, Оператор обязуется направить заблаговременно, по Согласованным каналам связи.

1.3. Оператор не устанавливает комиссию за участие в Платежной системе.

1.4. Оператор устанавливает комиссию за исполненное распоряжение Участника.

2. Общие принципы взимания комиссии с Отправителей:

2.1. Комиссия взимается в полном объеме Банком-Отправителем;

2.2. Комиссия взимается сверх суммы Перевода и в Валюте приема распоряжения на Перевод денежных средств;

2.3. Комиссия выражена в % соотношении от суммы Перевода;

2.4. Размер комиссии зависит от географического направления, суммы Перевода, способа отправления и маршрута расчетов, связанных с оказанием Услуг по осуществлению Перевода.

2.5. Банк Отправитель самостоятельно устанавливает размер взимаемой комиссии с Отправителя:

- за осуществление Перевода в сумме не большую чем **10% от суммы Перевода** за каждое исполненное распоряжение на Перевод на территории Российской Федерации;
- за осуществление трансграничного Перевода в сумме не более чем **20% от суммы Перевода** за каждое исполненное распоряжение на Перевод.

3. Порядок определения комиссионного вознаграждения Участников, в т.ч. порядок оплаты услуг платежной инфраструктуры.

3.1. Размер комиссионного вознаграждения Участников определяется Оператором, за исключением вознаграждения Участника, использующего право самостоятельного установления тарифов для Отправителей в соответствии с п. 2.4 настоящего Порядка.

3.2. Комиссия, взимаемая Банком-Отправителем с Отправителей, распределяется следующим образом:

- вознаграждение Банка-Отправителя остается в его распоряжении, если иное не предусмотрено соответствующим договором с Оператором;
- вознаграждение Оператора перечисляется Участником, обслуживающим Отправителя (т.е. инициирующего операцию);

3.3. Процедуры расчета комиссии осуществляются Оператором в рамках общих процедур клиринга и расчетов, в частности, комиссии включаются в платежную клиринговую позицию по каждому Участнику.

3.4. Оплата комиссии Оператору, по распоряжению Участника, осуществляется путем направления распоряжения в Расчетный центр для зачисления комиссионного вознаграждения на банковский счет Оператора.

4. Оплата комиссии за оказание услуг Расчетного центра, Операционного центра и Платежного клирингового центра в рамках расчетов с Платежной системой Участниками не осуществляется.

5. Услуги Расчетного центра Платежной системы, оплачиваются Оператором на основании условий договора о привлечении Расчетного центра, заключенного между Оператором и Расчетным центром.

6. Услуги Операционного центра и Платежного клирингового центра Платежной системы, оплачиваются Оператором на основании условий договора о привлечении Операционного центра и Платежного клирингового центра, заключенного между Оператором и Операционным центром, Оператором и Платежным клиринговым центром (при их наличии).

Т А Р И Ф Ы
Платежной системы «МОМЕНТОМ»

Наименование комиссии	***Размер тарифа***	***Получатель вознаграждения***
Операционное обслуживание операций по Переводу денежных средств Участников-Отправителей на территории Российской Федерации ***(уплачивается Банком Отправителем)***:	от 1,5% до 5% (минимум 15р.)	Оператор
Операционное обслуживание операций по трансграничному Переводу денежных средств Участников-Отправителей ***(уплачивается Банком Отправителем)***:		
- по уникальному идентификатору (абонентский номер, номер электронного средства платежа и т.д.)	от 3% до 10% (минимум 15р.)	Оператор
- по банковским реквизитам	от 3% до 10% (минимум 400р)	Оператор

Приложение № 3
к Правилам Платежной системы «МОМЕНТОМ»

Пороговые уровни показателей БФПС Платежной системы «МОМЕНТОМ»

		Пороговые уровни показателей	**Пороговые уровни показателей**	**Пороговые уровни показателей ПС «МОМЕНТОМ»**
		для каждого из ОУПИ системно и социально значимых ПС	*для каждого из ОУПИ ПС, не являющихся системно или социально значимыми*	
Показатель продолжительности восстановления оказания УПИ	**П1**	**не более** **2 часов**	**не более** **6 часов**	**не более** **6 часов**
		для каждого из ОУПИ системно значимой ПС	*для каждого из ОУПИ социально значимой ПС*	
Показатель непрерывности оказания УПИ	**П2**	**не менее 24 часов**	**не менее 12 часов**	**не менее 12 часов**
		для операционного и платежного клирингового центров ПС (и для ПС, в которых РЦ является ОЦ и/или ПКЦ)	*для расчетного центра ПС*	
Показатель соблюдения регламента	**П3**	**не менее 98,0%**	**не менее 99,0%**	**РЦ - не менее 99,0%** **ОЦ, ПКЦ - не менее 98,0%**

		для системно значимой ПС	*для социально значимой ПС*	*для ПС, не являющимися системно или социально значимыми*	

Показатель доступности операционного центра платежной системы	**П4**	**не менее 99,0%,**	**не менее 98,0%**	**не менее 96,0%**	**не менее 96,0%**
Показатель изменения частоты инцидентов	**П5**				**не более 1330,0% - если за предыдущий период было не более 5 инцидентов;** **не более 200,0% - если за предыдущий период было более 5 инцидентов.**

Приложение №4
к Правилам Платежной системы «МОМЕНТОМ»

Форма для оперативного информирования Оператора Платежной системы о выявленных инцидентах информационной безопасности

1.	Дата возникновения инцидента		
2.	Дата выявления инцидента		
3.	Место выявления инцидента		
4.	Время, прошедшее с момента обнаружения до момента блокировки инцидента		
5.	Указать признаки, по которым был выявлен инцидент		
6.	Условия возникновения инцидента (что могло спровоцировать инцидент)		
7.	Подробное описание инцидента		
8.	Причина инцидента		
9.	Причина, почему инцидент не был предотвращен штатными средствами безопасности		
10.	Дополнительная информация об инциденте		
11.	Нарушенное требование Положения №821-П		
12.	Последствия инцидента	Суммы переводов денежных средств	
13.		Нарушение сроков	
14.		Оценка убытка	
15.	Описание предпринятых действий по устранению последствий инцидента		
16.	Факт обращения в правоохранительные органы		
17.	Дата завершения разбирательства по инциденту		

Исполнитель _____ _____
(личная подпись) (инициалы, фамилия)

Номер телефона: _____

Приложение № 5

к Правилам Платежной системы «МОМЕНТОМ»

Бизнес-процессы Платежной системы «МОМЕНТОМ»

Бизнес-процессы	Процедуры	Код
Бизнес процессы присущие ОЦ: Операционные услуги	Получение и передача распоряжений Участников	1.001
	Получение и передача подтверждений об исполнении/извещений об отказе в исполнении распоряжений Участников	1.002
Бизнес процессы присущие ПКЦ: Услуги платежного клиринга	Прием к исполнению распоряжений Участников	2.001
	Процедуры контроля распоряжения: - проведение процедур удостоверения права распоряжения денежными средствами; - контроль целостности распоряжений; - структурный контроль распоряжений; - контроль дублирования распоряжений; - контроль значений реквизитов распоряжений; - контроль достаточности денежных средств	2.002
	Формирование и отправка принятых и обработанных распоряжений Участников	2.003
	Направление извещений об отказе в исполнении с указанием причин распоряжений Участников	2.004.
	Формирование платежно-клиринговой позиции Участников	2.005
	Передача Реестра нетто позиций Участникам и Расчетному центру	2.006
Бизнес-процессы присущие РЦ: Расчетные услуги	Исполнение распоряжений Участников	3.001.
	Направление подтверждений об исполнении распоряжений	3.002

Приложение № 6
к Правилам Платежной системы «МОМЕНТОМ»

ПРОФИЛЬ _____ РИСКА

(правового, операционного, кредитного, ликвидности, общего коммерческого, системного)

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1		1.1.							1.1.								

Далее указаны профили рисков в разрезе, определенных в нормативных документах Банка России и настоящих Правилах Платежной системы.

Профиль каждого из значимых рисков в Платежной системе «МОМЕНТОМ» содержит:

- описание риск-событий, выявленных с применением не менее чем одного метода из числа предусмотренных таблицей А.2 приложения А к Стандарту. Риск-события отражаются в профиле каждого из значимых рисков в Платежной системе «МОМЕНТОМ»;
- описание причины возникновения каждого из риск-событий;
- описание бизнес-процессов, в которых могут произойти риск-события;

- вероятность наступления риск-событий, определение вероятности наступления риск-событий осуществляется с применением не менее одного метода из числа предусмотренных Стандартом;

- описание и оценку 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;

- описание бизнес-процессов и перечень Субъектов Платежной системы, на которые влияет риск-событие;

- уровень присущего риска до применения способов управления рисками в Платежной системе;

- уровень допустимого риска, указанный в абзаце третьем четвертого предложения подпункта 8.3.12 настоящих Правил;

- уровень остаточного риска после применения способов управления рисками в Платежной системе;

- перечень способов управления рисками в Платежной системе.

Перечни риск-событий, указанные в профилях риска, не являются исчерпывающими, могут быть изменены и дополнены.

ПРОФИЛЬ ПРАВОВОГО РИСКА

(правового, операционного, кредитного, ликвидности, общего коммерческого, системного)

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Правовой**	1.1. Претензии правового характера к Субъектам ПС со стороны государственных органов из-за нарушения Субъектами Платежной системы требований законодательства РФ, нормативных актов Банка России	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Нарушение Субъектами Платежной системы требований законодательства РФ, нормативных актов Банка России из-за незнания или неверной трактовки законов РФ, норматив	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы				

			ых актов Банка России, правовые коллизии													
	1.2. Претензии правового характера к Субъектам ПС со стороны Оператора ПС из-за нарушения Субъектами ПС Правил	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Нарушение Субъектами ПС Правил из-за незнания или неверной трактовки Правил, нарушения требований Правил	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы				
	1.3. Претензии правового характера к Субъектам ПС со стороны других Субъектов ПС из-за нарушения договоров, заключенных между Субъектами	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Нарушение договоров, заключенных между Субъектами и Платежной системы из-за незнания, неверной трактовки договоров, нарушения требований договоров, в том числе вследствие нахождени	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы				

				я их под юрисдикцией различных государств													
		1.4. Претензии правового характера к Субъектам ПС со стороны других Субъектов ПС из-за нарушения документов Оператора и Операторов УПИ	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Нарушение Субъектами Платежной системы документов Оператора и Операторов УПИ из-за незнания или неверной трактовки документов, нарушения требований документов	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы				

ПРОФИЛЬ ОПЕРАЦИОННОГО РИСКА

(правового, операционного, кредитного, ликвидности, общего коммерческого, системного)

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	**Операционный**	2.1. Отказы и аварии в работе информационных и технологических Субъектов ПС	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	-Сбои оборудования; - Воздействие вредоносного кода; - Хакерские атаки	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы				
		2.2. Нарушение функционирования ПС из-	Синдинический подход, метод индексов риска и	- Нарушение выполнения технологических и управленче	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода			Синдинический подход, метод индек	Согласно Приложению № 5 к настоя	Субъект(ы) Системы				

		за недостатков в организации и выполнении технологических или управленческих процессов	элементы метода экспертных оценок	ских процессов; - Недостатки организации и технологических и управленческих процессов; - Нарушения информационной безопасности				экспертных оценок			сов риска и элементы метода экспертных оценок	щим Правилам					
		2.3. Нарушение функционирования ПС в результате ошибочных или противоправных действий персонала Субъектов ПС	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	- Ошибочные действия персонала; - Противоправные действия персонала; - Нарушения информационной безопасности	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы				
		2.4. Нарушение	Синдинический подход,	Внешнее воздействие	Согласно Приложени	Субъект Системы	0.5	Синдинический подход, метод			Синдинический	Согласно	Субъект(ы)	средний			

		функционирования ПС в результате ошибочных или противоправных действий третьих лиц	метод индексов риска и элементы метода экспертных оценок		ю № 5 к настоящим Правилам			индексов риска и элементы метода экспертных оценок			подход, метод индексов риска и элементы метода экспертных оценок	Приложению № 5 к настоящим Правилам	Системы				
		2.5. Нарушение функционирования ПС в результате последствий воздействия событий, причины возникновения котор	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Внешнее воздействие, катастрофы, пандемии	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы				

		ых связаны с деятельностью Субъектов ПС, включая чрезвычайные ситуации															

ПРОФИЛЬ КРЕДИТНОГО РИСКА

(правового, операционного, кредитного, ликвидности, общего коммерческого, системного)

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последсвий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

3	**Кредитный**	3.1. Несвоевременность проведения расчетов, задержка исполнения расчетных документов из-за невыполнения Участниками ПС договорных обязательств перед РЦ в установленный срок или в будущем	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	- Отзыв лицензии; - Санкционный список; - Предписание Банка России, введение ограничений или процедур оздоравления	Согласно Приложению № 5 к настоящим Правилам	РЦ, Участники		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы					

ПРОФИЛЬ РИСКА ЛИКВИДНОСТИ

(правового, операционного, кредитного, ликвидности, общего коммерческого, системного)

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

4	**Ликвидности**	4.1. Несвоевременность проведения расчетов, задержка исполнения расчетных документов из-за отсутствия у Участников ПС денежных средств, достаточных для своевременного выполнения их обязательств	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	- Несвоевременное пополнение счета Участника в РЦ; - Несвоевременное пополнение Участником счета в РЦ	Согласно Приложению № 5 к настоящим Правилам	РЦ, Участники		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы					

ПРОФИЛЬ ОБЩЕГО КОММЕРЧЕСКОГО РИСКА

(правового, операционного, кредитного, ликвидности, общего коммерческого, системного)

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18

5	**Общий коммерческий**	5.1. Ухудшение финансового состояния Оператора и/или Операторов УПИ, не связанного с реализацией кредитного риска и риска ликвидности ПС	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	- Неконкурентноспособность; - Потеря деловой репутации	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы					

ПРОФИЛЬ СИСТЕМНОГО РИСКА

(правового, операционного, кредитного, ликвидности, общего коммерческого, системного)

№	Профиль риска	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последствий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
6	**Системный**	6.1. Распространение между Субъектами ПС последствий сочетания двух или нескольких рисков, указанных выше, и вызыв	Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Реализация одновременно двух или нескольких рисков, указанных выше	Согласно Приложению № 5 к настоящим Правилам	Субъект Системы		Синдинический подход, метод индексов риска и элементы метода экспертных оценок			Синдинический подход, метод индексов риска и элементы метода экспертных оценок	Согласно Приложению № 5 к настоящим Правилам	Субъект(ы) Системы				

		ающих нарушения функционирования ПС															

+

ПРОФИЛЬ РИСКА НАРУШЕНИЯ БФПС

№	Профили рисков	Описание риск-события	Применяемый метод выявления риск-события	Причины (источники) возникновения риск-события	Бизнес-процесс, в котором произошло риск событие	Субъект Системы, являющийся владельцем бизнес-процесса	Вероятность наступления риск-события	Применяемый метод определения вероятности наступления риск-события	Описание последсвий риск-события	Оценка последствий риск-события	Применяемый метод оценки последствий риск-события	Бизнес-процессы, на которое влияет риск-событие	Субъекты Системы, на которые влияет риск-событие	Уровень присущего риска	Уровень допустимого риска	Применяемые способы управления рисками	Уровень остаточного риска
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	**Профиль правового риска**	1.1.							1.1.								
2	**Профиль операционного риска**	2.1.							2.1.								
3		3.1.							3.1.								

	Профиль кредитного риска																
4	**Профиль риска ликвидности**	4.1.							4.1.								
5	**Профиль общего коммерческого риска**	5.1.							5.1.								
6	**Профиль системного риска**	6.1.							6.1.								

Профиль риска нарушения БФПС составляется как сводный профиль в отношении всех значимых рисков в Платежной системе, указанных в абзаце четвертом четвертого предложения подпункта 8.3.12 настоящих Правил.

Приложение №7
к Правилам Платежной системы «МОМЕНТОМ»

Сведения о переводах в результате НСД к объектам его инфраструктуры

Раздел 1.1: Сведения о переводах в результате НСД к объектам его инфраструктуры

Номер строки	Последствия осуществления несанкционированного доступа	Количество событий, связанных с несанкционированным доступом, единицы	Сумма списанных денежных средств, тыс. руб.	Сумма операционных расходов оператора по переводу денежных средств в результате списаний денежных средств, тыс. руб.
1	2	3	4	5
Осуществление перевода денежных средств оператора по переводу денежных средств или его клиентов без их согласия в результате:				
1	несанкционированного доступа работников оператора по переводу денежных средств или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, к автоматизированным банковским системам (информации о банковских счетах)			X
2	Реализации компьютерных атак или несанкционированного доступа лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств, к автоматизированным банковским системам (информации о банковских счетах)			X
3	Итого			

Раздел 1.2: Сведения о неоказании услуг по переводу ДС

Номер строки	Причина неоказания услуг по переводу денежных средств	Количество событий, связанных с неоказанием услуг по переводу денежных средств, единицы	Регион неоказания услуг по переводу денежных средств (ОКАТО)
1	2	3	4
Неоказание услуг по переводу денежных средств на период более двух часов в целом по всем субъектам Российской Федерации, в которых оператор по переводу денежных средств осуществляет перевод денежных средств, с использованием систем (средств) дистанционного банковского обслуживания в результате:			
1	Реализации компьютерных атак работниками оператора по переводу денежных средств или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств		X
2	реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств		X
3	Итого		X
Неоказание услуг по переводу денежных средств на период более двух часов в целом по отдельным субъектам Российской Федерации, в которых оператор по переводу денежных средств осуществляет перевод денежных средств с использованием систем (средств) дистанционного банковского обслуживания в результате:			
4	Реализации компьютерных атак работниками оператора по переводу денежных средств или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств		
5	реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры оператора по переводу денежных средств		
6	Итого		X
7	Итого по разделу 1.2		X

Раздел 2.1: Сведения от Участников о списании ДС с коррсчетов без их согласия

Номер строки	Причина осуществления списаний денежных средств с корреспондентских счетов участников платежной системы	Регистрационный номер оператора платежной системы	Регистрационный номер кредитной организации	Сумма денежных средств, в отношении которой получено уведомление (оспаривание) от участников платежной системы, тыс. руб.	Сумма денежных средств, возмещенная участникам платежной системы, тыс. руб.
1	2	3	4	5	6
1	Исполнение распоряжений платежных клиринговых центров и участников платежной системы				
2	Несанкционированный доступ работников расчетного центра или иных лиц, обладающих полномочиями доступа к объектам информационной инфраструктуры расчетного центра, к информации о корреспондентских счетах участников платежной системы				
3	Реализация компьютерных атак или несанкционированный доступ лиц, не обладающих полномочиями доступа к объектам информационной инфраструктуры расчетного центра, к информации о корреспондентских счетах Участников платежной системы				
4	Итого по разделу 2.1	X	X		

Раздел 2.2: Сведения РЦ о неоказании расчетных услуг

Номер строки	Причины неоказания расчетных услуг	Количество событий, связанных с неоказанием расчетных услуг, единицы
1	2	3
Неоказание расчетных услуг на период более одного операционного дня в результате:		
1	реализации компьютерных атак работниками расчетного центра или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры расчетного центра	
2	реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры расчетного центра	
3	Итого	
Невыполнение в течение операционного дня расчетов для принятых к исполнению распоряжений платежного клирингового центра или участников платежной системы в результате:		
4	реализации компьютерных атак работниками расчетного центра или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры расчетного центра	
5	реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам информационной инфраструктуры расчетного центра	
6	Итого	
7	Итого по разделу 2.2	

1. Раздел 2.3: Сведения ОЦ о неоказании операционных услуг

Номер строки	Причины неоказания операционных услуг	Количество событий, связанных с неоказанием операционных услуг, единицы
1	2	3
Прерывание оказания операционных услуг на период более двух часов в результате:		
1	реализации компьютерных атак работниками операционного центра или иными лицами, обладающими полномочиями доступа к объектам информационной инфраструктуры операционного центра	
2	Реализации компьютерных атак лицами, не обладающими полномочиями доступа к объектам	
	Информационной инфраструктуры операционного центра	
3	Итого по разделу 2.3	

Руководитель _____ _____
(личная подпись) (инициалы, фамилия)

М.П.

Исполнитель _____ _____
(личная подпись) (инициалы, фамилия)

Номер телефона: _____