ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ
«Грин Телеком Сервис»

Утверждено постановлением
Правления № 5 от 16 декабря 2020 г.

Правила платежной системы «О!Деньги»

г. Бишкек

Оглавление:

1. ИНФОРМАЦИЯ ОБ ОПЕРАТОРЕ ПЛАТЕЖНОЙ СИСТЕМЫ (ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ)

1.1. Оператором платежной системы (совмещает свою деятельность с деятельностью Платежной организации) является Общество с ограниченной ответственностью «Грин Телеком Сервис» (ИНН 00411200910311, ОКПО 26738513, адрес: 720040, Кыргызская Республика, г. Бишкек, ул.

Абдрахманова, 170/2, блок 2).

1.2. Общество с ограниченной ответственностью «Грин Телеком Сервис» осуществляет свою деятельность на основании лицензии платёжной организации на оказание услуг по приему и проведению платежей и расчетов за товары и услуги, не являющиеся результатом своей деятельности, в пользу третьих лиц посредством платежных систем, основанных на информационных технологиях и электронных средствах, и способах проведения платежей. №3022030817 и лицензии оператора платежной системы на оказание услуг по приему, обработке и выдаче финансовой информации (процессинг, клиринг) по платежам и расчетам третьих лиц участникам платежной системы, данного процессингового, клирингового центра №2021030817, выданных Национальным Банком Кыргызской Республики 03 августа 2017 года.

1.3. Телефонный номер Оператора платежной системы (Платежной организации): +996 312 973-032

1.4. E-mail Оператора платежной системы (Платежной организации): dengi@dengi.kg

1.5. Номер call-центра Оператора платежной системы (Платежной организации): **+996 700-000-999, *999, *799 (для терминальной сети).**

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Абонент — физическое или юридическое лицо, заключившее с Поставщиком услуг Абонентский договор.

Абонентский договор – договор розничной купли-продажи Товаров, возмездного оказания Услуг, выполнения работ, заключенный в установленной форме с Поставщиком товаров/услуг.

Гарантийный взнос, Гарантийный платеж - денежные средства, переданные Платежным агентом Оператору платежной системы (Платежной организации), и/или Оператором платежной системы (Платежной организацией) Поставщику товаров/услуг или банку-эмитенту электронных денег, с целью страхования возможных рисков и обеспечения исполнения обязательств Платежного субагента перед Оператором платежной системы (Платежной организацией) или Оператора платежной системы (Платежной организации), перед Поставщиком товаров/услуг или банком-эмитентом электронных денег.

Гарантийный фонд – общая сумма, внесенных Платежным агентом и/или Оператором платежной системы (Платежной организацией) гарантийных взносов, за вычетом сумм, удержанных Оператором платежной системы (Платежной организацией) или Поставщиком товаров/услуг, в соответствии с условиями договора.

Дополнительное вознаграждение – сумма денежных средств в размере, определенном соглашением между Платежным агентом и Плательщиком, с учетом ограничений, установленных Оператором платежной системы (Платежной организацией), взимаемая Платежным субагентом с Плательщика при приеме Платежа и поступающая в распоряжение, соответственно, Платежного субагента.

Пользовательский интерфейс — в тексте настоящих Правил — программное обеспечение (установленное на Платежный терминал, мобильный телефон либо доступное через веб-интерфейс, а также посредством USSD- и SMS-запросов) - часть платежной **системы «О!Деньги»**, позволяющая учитывать Платежи, проводить разрешённые операции с электронными деньгами и передавать информацию о них на сервер Системы «О!Деньги».

Инцидент – это любое событие, которое не является частью штатного функционирования системы и вызывает или может негативно отразиться на бесперебойности или качестве проведения платежей и расчетов в платежной системе.

Лицевой счет Абонента - аналитический счет в автоматизированной системе расчетов Поставщика товаров/услуг, служащий для учета объема реализованного товара, оказанных услуг, выполненных работ, а также для учета поступления и расходования денежных средств, внесенных по договору с Поставщиком товаров/услуг.

Личный кабинет Платежного Агента - раздел web-интерфейса Системы «О!Деньги», содержащий реквизиты Платежного субагента, контактную информацию, параметры электронного документооборота, статистику, отчетность и другую информацию, необходимую для исполнения настоящих Правил.

Меры ПФТД/ЛПД – мероприятия, проводимые в целях соблюдения законодательства по противодействию финансирования террористической деятельности и легализации (отмыванию) преступных доходов

МПА - мобильное приложение агента Оператора/Оператора, используемое для проведения платежей, с использованием денежных средств, возвращаемых плательщику в счет ранее внесенных на его лицевой счет, открытый у поставщика товаров/услуг, авансов/предоплаты или их частей

Оператор платежной системы (Платежная организация), (Оператор) – Общество с ограниченной ответственностью «Грин Телеком Сервис», выполняющая функции координации и обеспечения деятельности Платежной Системы в целом.

Пользователь – идентифицированный (обязательное требование с 1 октября 2020 года) пользователь приложения О!Деньги

Платеж – исполнение обязательств по передаче денежных средств, внесенных Плательщиком в пользу Поставщика услуг, в целях исполнения обязательства по оплате товаров, услуг, работ (в том числе, внесение авансового платежа).

Платежный Агент/ (Агент) – юридическое лицо или индивидуальный предприниматель, включая его пункты приема платежей, осуществляющее деятельность по приему платежей, заявившее о присоединении к Правилам и подписавшее Договор присоединения к Правилам, (Агентский договор на осуществление деятельности по приему платежей), при условии, что данное лицо принимает условия Правил в целом, в соответствии со ст.387 Гражданского кодекса Кыргызской Республики.

Автоматизированный терминал самообслуживания (Платежный терминал) - устройство для приема денежных средств от Плательщика, функционирующее в автоматическом режиме.

Плательщик – дееспособное физическое лицо, заключившее с Оператором Системы Договор от своего имени или от имени юридического лица, путем присоединения к нему и имеющее право использовать Систему, в целях исполнения своих денежных обязательств и/или денежных обязательств юридического лица перед Поставщиком.

Подсистема «Агент» (ПА) - автоматизированное программное обеспечение и комплекс отношений (юридических, технических, информационных), возникающих в процессе организации и осуществления посреднической деятельности, связанной с приемом платежей (кроме платежей с использованием электронных денег) в целях исполнения (прекращения) денежных обязательств одних лиц перед другими, вместе образующих отдельную подсистему, входящую в состав системы «О!Деньги», которая обеспечивает информационное и технологическое взаимодействие между Оператором платежной системы (Платежной организацией), Платежными субагентами и Поставщиками услуг при приеме Платежей (без использования электронных денег), а также при обработке и передаче информации о платежах. Координация и обеспечение деятельности Подсистемы «Агент» обеспечивается Оператором Платежной Системы (Платежной организацией).

Поставщик товаров/услуг (Поставщик) - юридическое лицо или индивидуальный предприниматель, заключивший с Абонентом договор на реализацию товара, оказание услуг и/или выполнение работ, получающий Платеж от Плательщика.

Процессинг – информационное (сбор, обработка и рассылка информации по производимым операциям, а также иные сопутствующие операции) и технологическое (управление общесистемными справочниками, ограничениями, реестрами и другой системной информацией, а также иные сопутствующие операции) взаимодействие между Участниками Системы приема платежей, а также информационное и технологическое взаимодействие Участников Платежной системы.

Платежная Система (Система) - автоматизированная платежная система **«О!Деньги»**, обеспечивающая информационное и технологическое взаимодействие между участниками платежного процессинга при приеме и проведении Платежей от Плательщиков, проведении разрешенных операций с электронными деньгами.

Тарифный план – установленные Оператором платежной системы (Платежной организацией) ставки вознаграждения Платежного агента, за осуществление юридических и иных действий, предусмотренных Правилами, а также ставки вознаграждения Оператора за действия, предусмотренные Правилами. Тарифный план устанавливается для Платежного агента при подписании агентского договора к Правилам, в дальнейшем Тарифный план и все его изменения будут отображаться в личном кабинете Платежного агента.

Участник Платежной Системы – лицо, участвующее в деятельности по приему и проведению Платежей от Плательщиков. Оператор платежной системы (Платежная организация) для целей Правил также является Участником Системы приема платежей.

Электронные деньги - денежная стоимость, которая хранится в электронном виде на программно-техническом устройстве (предоплаченные карты, виртуальные предоплаченные карты и электронный кошелек являются инструментами (носителями) электронных денег) и принимаются в качестве средства платежа за товары/услуги.

Электронный кошелек - хранилище электронных денег, представляющее собой программное обеспечение или иное программно-техническое устройство, в котором имеется запись о сумме электронных денег и их принадлежности держателю.

ID номер лицевого счета – идентификационный номер (ID), присваиваемый лицевому счету Платежного агенту/субагента, как участнику Платежной системы (ПС).

3. ОБЩИЕ ПОЛОЖЕНИЯ

3.1. Настоящие Правила платежной системы «О!Деньги» (далее – «Правила») определяют единые условия осуществления деятельности общества с ограниченной ответственностью «Грин Телеком Сервис» и устанавливают стандартные права, обязанности и ответственность Участников Платежной Системы «О!Деньги».
Участниками Правил являются Оператор платежной системы (Платежная организация), Платежные агенты/субагенты, Поставщики товаров/услуг, пользователи. Платежным агентом/субагентом может стать любой индивидуальный предприниматель или юридическое лицо, заявившие о присоединении к Правилам и подписавшие соответствующий договор, при условии, что данное лицо принимает условия Правил в целом, в соответствии со ст.387 Гражданского кодекса Кыргызской Республики. Каждая из Сторон гарантирует другим Сторонам, что обладает необходимой правоспособностью, а равно всеми правами и полномочиями, необходимыми и достаточными для присоединения к Правилам и исполнения

обязательств в соответствии с их условиями.

3.2. Настоящие Правила регламентируют порядок и условия функционирования Системы, взаимодействие Участников, устанавливают правовые и организационные основы построения и функционирования Системы, условия и порядок присоединения к Системе, условия и порядок предоставления и использования Услуг Системы в целях проведения Платежей, а также иные положения, необходимые для функционирования Системы. Контроль за соблюдением Правил Системы Участниками осуществляет Оператор.

3.3. В рамках контроля за соблюдением Правил в соответствии с требованиями законодательства Оператор:

- контролирует соблюдение действующих правил и процедур, а также их соответствие требованиям законодательства Кыргызской Республики;
- предъявляет требования к необходимым техническим и программным средствам для проведения платежей другим Участникам платежной системы;
- ведет базу данных по Агентам, Субагентам и Поставщикам товаров/услуг платежной организации
- оценивает и управляет рисками в платежной системе;
- обеспечивает безопасное функционирование средств обработки информации;
- обеспечивает единый подход к управлению инцидентами и ведет реестр инцидентов;
- обеспечивает своевременное доведение информации по принятым в систему Платежам до Поставщика товаров/услуг при возникновении нештатной ситуации в соответствии с условиями договора и требованиями нормативных правовых актов Национального банка КР.

3.4. В случае вступления в силу изменений в нормативных правовых актах, регулирующих деятельность Оператора, положения которых противоречат изложенным в настоящих Правилах, включая Приложения, применяются вступившие в силу законодательные нормы.

4. ПОРЯДОК ПОДКЛЮЧЕНИЯ УЧАСТНИКА К ПЛАТЕЖНОЙ СИСТЕМЕ

4.1. Настоящие Правила являются неотъемлемой и составной частью Договора, заключенного с Участником Системы, и безотзывно признаются Участниками обязательными к исполнению в полном объеме без каких-либо изъятий и исключений.

4.2. Оператор, при заключении договоров и формировании базы данных по Агентам, Субагентам и Поставщикам товаров/услуг, получает от Участника обязательные сведения:

- наименование юридического лица/ФИО индивидуального предпринимателя;
- данные о государственной регистрации юридического лица, паспортные данные индивидуального предпринимателя, патент, свидетельство о регистрации;
- местонахождение /адрес проживания, адрес осуществления предпринимательской деятельности;
- сведения о руководителях;
- контактные данные;
- сведения о собственниках/ учредителях (для юридических лиц);
- сведения о бенефициарных собственниках Поставщиков товаров/услуг;
- сведения о виде деятельности юридического лица/индивидуального предпринимателя (банковская деятельность, коммунальные услуги и т.д.);

- актуальный список адресов, где установлены терминалы (данная информация должна обновляться ежемесячно в период действия договора) агентов/субагентов.

4.3. Порядок заключения договора с Поставщиками товаров/услуг

4.3.1. При заключении Договора с Поставщиком товаров/услуг, Поставщик товаров/услуг предоставляет Оператору копии следующих документов:
- Устав;
- Учредительный договор (если имеется);
- Решение о создании (или о перерегистрации) юридического лица;
- Решение о назначении/избрании исполнительного органа юридического лица;
- Паспорт руководителя юридического лица;
- Свидетельство о Государственной регистрации;
- Если деятельность Поставщика товаров/услуг является лицензируемой, то копию соответствующей лицензии;
- Сведения о бенефициарных собственниках в соответствии с требованиями законодательства Кыргызской Республики.

Все копии вышеперечисленных документов заверяются подписью руководителя и скрепляются печатью юридического лица.

4.3.2. В случае если Поставщик является индивидуальным предпринимателем, то предоставляются копии следующих документов:
- Паспорт индивидуального предпринимателя;
- Свидетельство о государственной регистрации индивидуального предпринимателя и Извещение Плательщику социальных взносов в Социальных фонд Кыргызской Республики; или
- Патент и страховой полис с приложением соответствующих квитанций об оплате;

Свидетельство о постановке на учет физического лица/индивидуального предпринимателя в налоговом органе по месту жительства на территории Кыргызской Республики при наличии (предоставляется лицами, занимающимися предпринимательской деятельностью.

4.3.3. В исключительных случаях для заключения Договора у Поставщика товаров/услуг могут быть запрошены иные документы.

4.3.4. При заключении Договора с Поставщиком товаров/услуг Стороны определяют:
- порядок и условия исполнения денежных обязательств Оператора перед Поставщиком товаров/услуг за принятые Оператором и/или его Агентами Платежи;
- порядок и условия подключения Поставщика товаров/услуг к Системе;
- Технический Регламент взаимодействия аппаратно-программных средств Оператора и Поставщика товаров/услуг;
- порядок предоставления данных (реестров Платежей) для проведения регулярных сверок информации о принятых Оператором и/или его Агентами Платежах на основе информации, содержащейся в аппаратно-программном комплексе Оператора и данных о принятых Оператором платежах, содержащихся в аппаратно-программном комплексе Поставщика;

4.3.5. Стороны производят интеграцию аппаратно-программных средств Оператора с аппаратно-программными средствами Поставщика товаров/услуг согласно принятому Сторонами Техническому Регламенту и Протоколу обмена данными;

4.3.6. После завершения интеграции, Оператор вносит в Систему необходимые данные для возможности приема платежей Поставщика товаров/услуг Оператором и/или его Агентами/Субагентами;

4.3.7. Оператор направляет уведомления Агентам о подключении к Системе нового Поставщика товаров/услуг с предоставлением информации (в том числе об условиях финансовых взаимоотношений между Оператором и Агентом по данному Поставщику товаров/услуг), объективно необходимой для приема Агентом Платежей в пользу Поставщика товаров/услуг;

4.3.8. Договор с Поставщиком товаров/услуг может иметь иные порядки и условия заключения Договора с Поставщиком товаров/услуг.

4.4. Порядок заключения Договора с Агентом и другими участниками Платежной Системы

4.4.1. До начала деятельности связанной с проведением Платежей Участник платежной системы обязан осуществить регистрацию в Платежной Системе путем подписания/присоединения к Договору Платежной Системы, по форме, установленной Оператором. Предоставление Оператору подписанного Договора /согласия о присоединении к Договору, соответствующей формы - является подтверждением, что Участник платежной системы согласен с Правилами и обязуется соблюдать условия Правил и Договора. После представления Оператору подписанного Договора Участника Платежной Системы/согласия о присоединении к Договору, Участник платежной системы не может ссылаться на то, что он не ознакомился с Правилами либо не признает их обязательность в договорных отношениях с Оператором.

4.4.2. Участник предоставляет Оператору копии документов, заверенные руководителем и скрепленной печатью организации, если Участник юридическое лицо:

- Устав юридического лица;
- Решение (либо протокол) о создании юридического лица;
- Свидетельство о государственной регистрации юридического лица в министерстве юстиции;
- Свидетельство о регистрации юридического лица в налоговом органе (с параметрами);
- Документ (решение, протокол) об избрании руководителя организации (Генерального директора, Директора);
- В случае если юридическое лицо действует через представителя, представляется доверенность уполномоченному представителю Платежного агента на подписание договора и/или иных документов (с указанием паспортных данных, даты выдачи и срока действия доверенности и с приложением паспорта доверенного лица);
- Сведения (копии паспортов и др. данные в соответствии с законодательством) о бенефициарных собственниках (если имеются);
- актуальный список адресов, где установлены Платежные терминалы, в случае их наличия.

4.4.3. Перечень документов для индивидуального предпринимателя:

- свидетельство о государственной регистрации и извещение плательщику страховых взносов;
- свидетельство о регистрации в налоговом органе (с параметрами);
- паспорт индивидуального предпринимателя;
- добровольный или обязательный патент и страховой полис с приложением квитанций об оплате;
- актуальный список адресов, где установлены Платежные терминалы, в случае их наличия..

4.4.4. После регистрации Участнику в Системе заводится лицевой счет, которому присваивается индивидуальный ID номер.

4.4.5. Оператор вправе отказать любому Участник в регистрации, а также отказаться от подписания Договора Участника Платежной Системы в случае несоответствия лица требованиям законодательства и настоящим Правилам.

5. ПРАВА, ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ УЧАСТНИКОВ ПЛАТЕЖНОЙ СИСТЕМЫ

5.1. Права и обязанности Оператора при взаимодействии с Поставщиками товаров/услуг:

5.1.1. Оператор вправе:

- Оператор по поручению и за счет Поставщика товаров/услуг вправе принимать платежи Плательщиков, как с использованием электронных кошельков и электронных денег, так и без, в том числе с использованием МПА, наличных и безналичных средств, и обязуется принятую оплату перечислять Поставщику товаров/услуг (или иным законным способом осуществлять расчеты с Поставщиком товаров/услуг) в порядке, предусмотренном настоящими Правилами, а также Договором с Поставщиком товаров/услуг, в свою очередь Поставщик товаров/услуг обязуется выплачивать Оператору вознаграждение, в порядке, предусмотренном настоящими Правилами и Договором с Поставщиком товаров/услуг, если такая выплата предусмотрена Договором с Поставщиком товаров/услуг. Размер вознаграждения определяется Договором с Поставщиком товаров/услуг;
- Оператор вправе принимать платежи лично или поручить принятие платежей третьим лицам - Агентам Оператора, оставаясь при этом полностью ответственным перед Поставщиком товаров/услуг;
- Оператор и/или Агенты Оператора вправе осуществлять прием (получение) платежей Плательщиков любыми, не запрещенными законодательством способами (наличными деньгами; безналичными средствами); а также посредством иных платежных систем и инструментов, не запрещенных законодательством Кыргызской Республики);

5.1.2. Обязанности Оператора:

- Подготовить программное обеспечение, позволяющее обеспечить, в соответствии с требованиями Технического Регламента взаимодействие аппаратно-программных средств Оператора с аппаратно-программными средствами Поставщика для целей обеспечения передачи Информации о Платеже;
- Зарегистрировать Поставщика в своей электронной базе и присвоить ему код получателя платежей;
- Обеспечить перечисление Платежей, принятых Оператором и/или Агентами Оператора в порядке исполнения Договора с Поставщиком, на основании данных Реестра принятых Оператором и/или Агентами Оператора Платежей, регулярными едиными консолидированными платежами. При этом, обязательства Оператора по перечислению Поставщику товаров/услуг, принятых в его пользу платежей считаются исполненными с момента списания соответствующей суммы денежных средств с банковского счета Оператора. Срок, в течение которого Оператор обязан произвести перечисление, принятых Оператором платежей, а также порядок перечисления, определяется Договором с Поставщиком;
- Оператор и Поставщик подписывают Акт сверки расчетов за отчетный период. Порядок и срок предоставления Акта, рассмотрения Акта и его подписания, определяются Договором с Поставщиком;

5.1.3. Оператор должен:

- Иметь процедуры по обеспечению безопасности и непрерывности функционирования рабочих станций персонала.
- Иметь процедуры по резервированию каналов связи по передаче данных.
- Иметь процедуры по обеспечению конфиденциальности, передаваемых и получаемых от платежной системы данных согласно законодательству Кыргызской Республики.
- Должен обеспечить соответствие мощности линий и другого оконечного оборудования, через которое осуществляется подача энергоснабжения для работы систем, требованиям систем по мощности.
- В случаях перебоев энергоснабжения, должен обеспечить автономное энергоснабжение систем.
- Иметь процедуры, регламентирующие время автономного функционирования системы, а также обеспечивающие выполнение требований по продолжительности автономной работы системы, с момента прекращения энергоснабжения и до момента последующего переключения на

резервный АПК системы.

- При сбоях аппаратного или программного обеспечения, должен обеспечить использование альтернативных и/или резервных средств в соответствии со своими внутренними процедурами.
- При сбое основного канала связи должен провести переключение на резервный канал связи в соответствии со своими внутренними процедурами.
- Для снижения риска возникновения внутреннего мошенничества, должен иметь систему защиты от мошенничества и несанкционированного доступа на уровне аппаратно-программного комплекса (использование паролей и прав доступа к системе, криптографии, шифрования и т.п.), квалифицированный персонал для работы в системе, а также утвержденные должностные инструкции, определяющие ответственность, права и обязанности персонала.
- В случае возникновения фактов внутреннего мошенничества, затрагивающих условия заключенного Договора, Стороны проводят внутреннее расследование по факту мошенничества, и письменно уведомляют друг друга о результатах данного расследования. Претензии сторон, возникшие в результате внутреннего мошенничества, решаются в рамках, установленных законодательством Кыргызской Республики.

5.1.4 В целях страхования возможных рисков Поставщиков товаров/услуг Оператор обеспечивает:

1) предоставление 100 (ста) процентов предоплаты на всю сумму, принимаемых платежей в бюджеты бюджетной системы Кыргызской Республики, с установлением данного требования в соответствующих договорных отношениях с уполномоченным государственным органом по прогнозированию и исполнению бюджета и реализацией необходимых механизмов контроля и управления рисками (при заключении прямых договоров) для осуществления приема денежных средств плательщиков по уплате налогов, сборов и платежей, подлежащих зачислению на Единый казначейский счет уполномоченного органа по прогнозированию и исполнению бюджета в Национальном банке Кыргызской Республики. В случае превышения суммы платежей над размером предоплаты услуга поставщика товаров/услуг должна автоматически отключаться;
2) размещение страхового депозита в размере 50 (пятьдесят) процентов среднедневного оборота за последний квартал по каждому поставщику товаров/услуг для поставщиков товаров/услуг, полностью или частично находящихся в государственной собственности, коммунальных предприятий и бюджетных организаций, где договорные отношения не предусматривают предоплату, безотзывную банковскую гарантию либо депозит, размещенный на банковском счете поставщика товаров/услуг.
В договоре с Поставщиком товаров/услуг предусматривается, что страховой депозит будет использоваться только по целевому назначению при наступлении случаев неисполнения/нарушения Оператором обязательств по перечислению принятых платежей на расчетный счет Поставщика товаров/услуг, а также условия контроля банковского счета, на котором размещен страховой депозит, и/или возможность безакцептного списания денежных средств Поставщиком товаров/услуг;
3) размещение на банковском счете по вкладам на иных условиях возврата в коммерческом банке страхового депозита либо представление Оператором безотзывной банковской гарантии в пользу Поставщика товаров/услуг для поставщиков товаров/услуг, где договорные отношения не предусматривают предоплату Поставщику товаров/услуг. Размер страхового депозита либо банковской гарантии должен составлять не менее 10 (десяти) процентов от суммы среднедневного оборота Оператора за последний квартал по каждому Поставщику товаров/услуг.

5.2. Права и обязанности Поставщика товаров/услуг.

5.2.1. Поставщик товаров/услуг обязан:

- Подготовить необходимое оборудование и программное обеспечение, позволяющее обеспечить взаимодействие с аппаратно-программными средствами Оператора в соответствии с требованиями

Технического Регламента;

- Для целей регистрации Поставщика товаров/услуг в электронной базе данных Оператора и корректного проведения платежей, а также для целей взаимодействия сторон в порядке исполнения Договора с Поставщиком товаров/услуг, сообщить Оператору сведения и предоставить документы, предусмотренные п.4 настоящих Правил;
- Уведомлять Оператора об изменениях в параметрах Платежей, которые могут повлиять на идентификацию Плательщика и в целом на корректность проведения Платежа в порядке и в сроки, определенные Договором с Поставщиком товаров/услуг;
- Контролировать и учитывать денежные средства Оператора, внесенные им (Оператором) в качестве предоплаты Поставщику товаров/услуг в счет будущих Платежей, проводимых Оператором;
- В случае ошибочного перечисления Оператором в пользу Поставщика товаров/услуг денежных средств, перечисленных Оператором в порядке исполнения обязательств Оператора перед Поставщиком товаров/услуг, которые (платежи) возникли в результате любой технической ошибки, возвратить Оператору по его письменному заявлению ошибочно перечисленные денежные средства в течение трех (3) банковских дней с момента получения соответствующего требования. Отдельные Договора с Поставщиками товаров/услуг могут содержать иные условия возврата ошибочно перечисленных Оператором денежных средств в пользу Поставщика товаров/услуг;
- В случае совершения ошибочного платежа по вине (в том числе, неосторожной) Плательщика (неверное указание номера лицевого счета, неверное указание суммы платежа, неверное указание номера телефона и т.п.), по письменному заявлению Оператора, возвратить Оператору ошибочно перечисленные денежные средства, либо изменить параметры платежа, если такой возврат и такое изменение параметров платежа возможны и имеется такая возможность;
- Согласовывать ежемесячный Акт сверки расчетов за соответствующий отчетный месяц путем его подписания. Порядок и срок получения ежемесячного Акта определяется Договором с Поставщиком товаров/услуг;
- Выплачивать Оператору вознаграждение в порядке и размере, установленном в Договоре с Поставщиком товаров/услуг, если такое вознаграждение предусмотрено Договором с Поставщиком товаров/услуг;

5.2.2. Поставщик товаров/услуг должен:

- Иметь в штате специалистов, выполняющих функции приема платежей (переводов), а также функции обмена другими сообщениями в рамках платежной системы.
- Иметь в штате специалистов по сопровождению системы, обеспечивающих бесперебойное функционирование и безопасность технической инфраструктуры.
- Иметь процедуры по обеспечению конфиденциальности передаваемых и получаемых от платежной системы данных согласно законодательству Кыргызской Республики.
- При сбое основного канала связи с Оператором должен провести переключение на собственный резервный канал связи в соответствии со своими внутренними процедурами.
- Для снижения риска возникновения внутреннего мошенничества должен иметь квалифицированный и прошедший проверку персонал для работы в системе, а также утвержденные должностные инструкции, определяющие ответственность, права и обязанности персонала.
- В случае возникновения фактов внутреннего мошенничества, затрагивающих условия настоящего заключенного Договора, Стороны проводят внутреннее расследование по факту мошенничества, и письменно уведомляют друг друга о результатах данного расследования. Претензии сторон, все спорные ситуации, возникшие в результате внутреннего мошенничества, решаются в рамках, установленных законодательством Кыргызской Республики.

5.2.3. Права Поставщика товаров/услуг:

- Требовать от Оператора своевременного исполнения финансовых обязательств, возникших у Оператора за прием Оператором и/или его Агентами Платежей Поставщика товаров/услуг;
- Требовать от Оператора выполнения надлежащим образом обязательств, предусмотренных

настоящими Правилами и Договором с Поставщиком товаров/услуг;

- В случае, если Оператор исполняет свои обязательства перед Поставщиком товаров/услуг по принципу предоплаты, Поставщик товаров/услуг вправе по надлежаще оформленному запросу Оператора предоставить кредитный лимит на совершаемые Оператором платежи, за исключением платежей в бюджеты бюджетной системы Кыргызской Республики. При этом Стороны определяют размер кредитного лимита, а также порядок и сроки его погашения, если иное не определено Договором с Поставщиком товаров/услуг. Риск по неоплате возникших в данном случае обязательств Оператора перед Поставщиком товаров/услуг берет на себя Поставщик товаров/услуг;

5.3. Права Оператора

5.3.1.

Требовать от Поставщика товаров/услуг выполнения надлежащим образом обязательств, предусмотренных настоящими Правилами и Договором с Поставщиком товаров/услуг;

5.3.2.

Требовать от Поставщика товаров/услуг выплаты причитающегося Оператору вознаграждения в порядке и в сроки, определенные Договором с Поставщиком товаров/услуг за принятые Оператором и/или Агентами Оператора Платежи, если такая выплата предусмотрена Договором с Поставщиком товаров/услуг;

5.3.3.

В случае совершения ошибочных платежей, корректировка и аннулирование (отмена) платежей производится в соответствии с процедурами (порядком), описанными в Договоре с Поставщиком товаров/услуг;

5.3.4.

Оператор и/или Агенты/Субагенты Оператора вправе взимать с Плательщиков в свою пользу плату за использование ресурсов аппаратно-программного комплекса (АПК) Оператора при приеме и обработке Платежей, размер которой (платы) определяется Договором с Поставщиком товаров/услуг.

5.3.5.

Стороны вправе размещать товарные знаки друг друга посредством использования собственных информационных ресурсов исключительно в целях рекламирования товаров (работ, услуг) владельцев товарных знаков;

5.4. Ответственность Сторон при взаимодействии Оператора с Поставщиком товаров/услуг

5.4.1.

Стороны несут ответственность за ненадлежащее исполнение своих обязательств в соответствии с положениями настоящих Правил, а также Договора с Поставщиком товаров/услуг, а в случаях, не предусмотренных Правилами и Договором - в соответствии с законодательством Кыргызской Республики;

5.4.2.

В случае нарушения Оператором обязательств по перечислению Поставщику товаров/услуг, принятых в порядке исполнения Договора с Поставщиком товаров/услуг Платежей, Оператор обязуется уплатить Поставщику товаров/услуг неустойку в размере, порядке и сроки, определенные в Договоре с Поставщиком товаров/услуг;

5.4.3.

В случае нарушения Поставщиком товаров/услуг порядка выплаты вознаграждения, предусмотренного в Договоре с Поставщиком товаров/услуг и/или в его соответствующих приложениях (сумма, сроки), Поставщик товаров/услуг обязуется выплатить Оператору штрафную неустойку в размере, порядке и сроки, определенные в Договоре с Поставщиком товаров/услуг;

5.4.4.

В случае временного приостановления или прекращения приема Платежей Оператором, в том числе, в связи с прекращением действия Договора с Поставщиком товаров/услуг, Поставщик товаров/услуг не вправе требовать, а Оператор не обязан возмещать Поставщику товаров/услуг какой-либо косвенный ущерб (упущенную выгоду, недополученные доходы (прибыль) и т.п.), если иное не предусмотрено Договором с Поставщиком товаров/услуг;

5.4.5.

Оператор не несет ответственности за несвоевременное перечисление Поставщику товаров/услуг принятых Платежей при несвоевременном сообщении Поставщиком товаров/услуг об изменении своих реквизитов, а также в случае сбоя в работе электронных систем обслуживающего банка;

5.4.6

Оператор не несет ответственности за ошибки, допущенные Плательщиком при совершении Платежа;

5.4.7 В случае причинения убытков любой из Сторон или любому третьему лицу в связи с нарушением требований Технического Регламента, то такие убытки должны быть возмещены в полном объеме пострадавшей Стороне и/или соответствующему третьему лицу Стороной, нарушившей требования Технического Регламента.

5.5 Права и обязанности Агента, другого Участника

5.5.1. Агент/ Участник обязан:

- Оплачивать услуги Процессинга Оператора платежной системы (Платежной организации) в отношении Поставщиков товаров/услуг, определенных в Личном кабинете Агента/ Участника.
- Любая операция по передаче данных о Платеже возможна только с помощью Системы «О!Деньги».
- Участника /Агент обязан передавать Оператору платежной системы (Платежной организации) в режиме реального времени данные о каждом принятом Платеже.
- Платежный агент обязан после приема Платежа предоставить Плательщику извещение, подтверждающее Платеж, в форме установленной действующим законодательством и Оператором.
- Внести до начала приема Платежей на расчетный счет Оператора Гарантийный взнос.
- Агент/ Участник обязан извещать Оператора платежной системы (Платежной организации) об изменении любых данных, указанных Агентом/ Участником при регистрации в Платежной Системе, в том числе юридического и фактического адреса, почтового адреса, адреса электронной почты, контактных телефонов, изменении уполномоченных представителей Агента/ Участника, изменении банковских реквизитов, переход Агента/ Участникана иной режим налогообложения и т.д. Извещение должно быть направлено Агентом/ Участникомпо электронной почте курирующему менеджеру в течение 3 (трех) дней с момента изменения соответствующих данных, а также приложено в письменном виде к Акту о выполнении работ за тот месяц, в котором произошли соответствующие изменения.
- Не компрометировать и не нарушать права на Товарные знаки Оператора.
- Своевременно информировать Оператора о наступлении, существовании, изменении любых обстоятельств, имеющих значение для исполнения настоящих Правил.
- В случае прекращения (приостановки) полномочий Агента/ Участника по пользованию Системой «О!Деньги», Агент/ Участник обязан немедленно прекратить прием Платежей и пользование Системой «О!Деньги», а также убрать все рекламные материалы.
- Агент/ Участник обязан осуществлять последующие расчеты с Оператором в соответствии с заключенным договором, настоящими Правилами и действующим законодательством.

- Предоставлять любую запрашиваемую Оператором информацию в части агентской деятельности, в том числе актуальный список адресов, где установлены Платежные терминалы (если таковые имеются);
- Обеспечить беспрепятственный доступ Национальному банку в целях проверки агентов и субагентов Оператора на соответствие требованиям нормативных правовых актов Национального банка и предоставления необходимых документов, связанных с проверкой деятельности, осуществляемой в качестве агента при наличии у представителей Национального банка документа, подтверждающего право проведение данной проверки.
- При наличии подозрения в осуществлении финансирования террористической деятельности и легализации (отмывания) преступных доходов и других предикатных преступлений вследствие проведения платежа/платежей провести идентификацию и верификацию плательщика

5.6 Агент/ Участник имеет право:

- Применять в рекламных целях Товарные знаки Оператора по письменному согласованию с Оператором. Товарные знаки в пользование Агента/ Участника не передаются.
- Взимать с Плательщика Дополнительное вознаграждение с учетом ограничений, установленных Оператором.

5.7 Права и обязанности Оператора при взаимодействии с Агентом/ Участником

5.7.1. Оператор обязан:

- После окончания регистрации Оператор обязуется предоставить Агенту логин и пароль Личного кабинета Агента/ Участника.
- Выплачивать Агенту/ Участнику вознаграждение, если иное не предусмотрено Договором с Агентом.
- Своевременно информировать Агента/ Участника о наступлении, существовании, изменении любых обстоятельств, имеющих значение для исполнения Правил.
- Оператор обязуется при заключении Договора Участника Платежной Системы определить ставки вознаграждения Агента/ Участника за прием Платежей в пользу соответствующих Поставщиков товаров/услуг разработать внутренние нормативные документы для обеспечения бесперебойного функционирования своей информационной системы и безопасности проведения платежей. Программные и технические средства, применяемые в системах расчетов должны соответствовать требованиям Национального банка по обеспечению информационной безопасности;
- Внедрить:
- организационные, процедурные меры и использование технических средств в целях выявления, а также предотвращения, препятствования и противодействия мошенничеству;
- систему защиты информации, которая должна осуществлять непрерывную защиту информации во время приема платежей и на всех этапах ее формирования, обработки, передачи и хранения в Системе;
- внутренний контроль в целях противодействия легализации (отмыванию) преступных доходов и финансированию террористической и экстремистской деятельности;
- Обеспечить фиксирование всех транзакций между участниками Системы;
- Хранить в течение пяти лет соответствующую информации о транзакциях в Системе в форме, которая дает возможность проверить ее целостность.

5.8 Оператор при взаимодействии с Агентом/ Участником имеет право:

5.8.1. При отсутствии денежных средств в остатке Гарантийного фонда приостановить техническую возможность принимать Платежи

5.8.2. Отказать в оказании услуг по настоящим Правилам в случаях, предусмотренных законодательством Кыргызской Республики и настоящими Правилами.

5.8.3. Проверять в любое время ход исполнения Агентом/ Участником обязательств, связанных с настоящими Правилами, не вмешиваясь в его хозяйственную деятельность.

5.8.4. Оператор вправе в одностороннем порядке вносить изменения в Правила путем публикации документа, содержащего информацию о таких изменениях на сайте Системы www.dengi.kg. Изменения вступают в силу по истечении 5 (пяти) рабочих дней с момента опубликования, если иной срок вступления изменений в силу не определен дополнительно при их публикации. Агент/ Участник обязуется либо принять изменение условий Правил, либо до момента вступления изменения условий Правил в силу предоставить Оператору ответ об отказе в принятии изменений условий Правил. В случае непредставления ответа об отказе принять предложение, предложение об изменении условий Правил считается акцептованным (принятым) Агентом/ Участником. В случае несогласия Агента/ Участника с изменениями в условиях Правил, стороны имеют право расторгнуть Договор Участника Платежной Системы, произведя предварительно все расчеты.

5.8.5. В случае неисполнения (ненадлежащего исполнения) Агентом/ Участником какого-либо из обязательств, предусмотренных настоящими Правилами, Оператор вправе без предварительного уведомления отключить/блокировать Агента/ Участника в Системе «О!Деньги» и в письменной форме потребовать немедленного устранения нарушений, а также возмещения убытков.

5.8.6. Требовать от Агента/ Участника поддержания остатка Гарантийного фонда не ниже прогнозируемой величины ежедневно принимаемой Агентом/ Участником суммы Платежей, и оставляет за собой право при отсутствии денежных средств в остатке Гарантийного фонда приостановить техническую возможность принимать Платежи.

5.8.7. В случае если требования об устранении нарушения не были выполнены Агентом/ Участником в течение 3 (трех) рабочих дней, Оператор вправе расторгнуть Договор Участника Платежной Системы в одностороннем порядке.

5.8.8. Уведомление о расторжении Договора Участника Платежной Системы по указанному выше основанию направляется Оператором Агенту/ Участнику в письменном виде. Полномочия Агента/ Участника по пользованию Системой «О!Деньги» прекращаются с момента уведомления Оператором Агента/ Участника, при этом Договор Участника Платежной Системы считается расторгнутым с момента уведомления Агента/ Участника.

5.8.9. Оператор в случаях заключения договора с новым Поставщиком товаров/услуг, либо изменения условий работы с Поставщиком товаров/услуг, либо по иным причинам указанным в настоящих Правилах, оставляет за собой право в одностороннем порядке изменить как перечень Поставщиков товаров/услуг, в пользу которых могут приниматься Платежи, так и ставки вознаграждения Агента/ Участника за прием Платежей конкретного Поставщика товаров/услуг, путем опубликования в Личном кабинете Агента/ Участника новости об внесений вышеперечисленных в настоящем пункте изменений. При этом изменения, внесенные в перечень Поставщиков товаров/услуг и Тарифные планы, вступают в силу для Агента/ Участника по истечении одних суток с момента размещения новости об изменениях в Личном кабинете Агента/ Участника, если иная дата вступления в силу не указана Оператором. Новые условия считаются принятыми (акцептованными) Агентом/ Участником при приеме им Платежей после даты вступления изменений в силу.

5.9. Ответственность сторон при взаимодействии Оператора и Агента/ Участника.

5.9.1. Стороны несут ответственность за ненадлежащее исполнение своих обязательств в соответствии с положениями настоящих Правил, а также Договора с Агентом/

Участником, а в случаях, не предусмотренных Правилами и Договором - в соответствии с законодательством Кыргызской Республики;

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

5.9.3. Агент/ Участник самостоятельно и за собственный счет разрешает спорные ситуации с Плательщиками, связанные с не прохождением Платежа в Системе «О!Деньги» в связи с отсутствием необходимого программного либо технического обеспечения, а также иными причинами, вызванными виновными действиями/бездействием Агента.

5.9.4. Агент/ Участник, в нарушение действующего законодательства не исполнивший обязательства, указанные в настоящих Правилах, несет установленные соответствующими нормативными правовыми актами меры ответственности, а также обязуется возместить убытки, возникшие у Оператора вследствие действий контролирующих органов, вызванных неисполнением Агентом/ Участником указанных обязанностей.

5.9.5. Оператор не несет ответственности за прямые или косвенные убытки Агента/ Участника, в том числе упущенную выгоду, понесенную сторонами по вине Оператора связи, включая временное снижение качества связи и (или) отказ оборудования сети.

5.9.6. Оператор не несет ответственности в случае несанкционированного доступа к Личному кабинету Агента/ Участника в Системе «О!Деньги» со стороны третьих лиц.

5.9.7. Стороны несут ответственность за действия своего персонала, связанные с нарушением положений настоящих Правил и/или Приложений к ним, если они повлекли неисполнение или ненадлежащее исполнение обязательств Сторон.

5.9.8. Взыскание любых неустоек и штрафных санкций, а также предъявление требования о возмещении убытков является правом, а не обязанностью, и реализуется Сторонами по собственному усмотрению.

5.9.9. Право Стороны на взыскание убытков, неустойки, штрафных санкций реализуется путем направления виновной стороне письменной претензии. Оператор вправе зачесть задолженность по всем денежным обязательствам Агента/ Участника в счет подлежащего выплате Агенту/ Участнику вознаграждения либо вычесть сумму задолженности из сумм Гарантийного фонда Агента/ Участника, а также применить претензионный порядок взыскания указанной задолженности.

5.9.10. Уплата штрафных санкций и возмещение убытков не освобождает Стороны от надлежащего выполнения принятых обязательств и соблюдения, настоящих Правил.

6. ПОРЯДОК РАЗРЕШЕНИЯ СПОРОВ, ЖАЛОБ УЧАСТНИКОВ

6.1. Все разногласия, возникающие в процессе исполнения Договора с Участниками, Стороны будут стремиться разрешить путем переговоров.

6.2. Любые неразрешенные путем переговоров споры, возникающие из настоящих Правил или из Договора с Участником в том числе касающиеся его нарушения, прекращения, расторжения или недействительности, подлежат разрешению в суде Кыргызской Республики, в соответствии с Применимым материальным правом Кыргызской Республики;

6.3. Порядок обработки обращений и жалоб Участников осуществляется в общем порядке:

1) Обработка всех обращений, принятых по звонку в Колл-центр
2) Обработка всех обращений, принятых по электронной почте и нарочно

6.4. При приеме обращений и жалоб обязательными условиями является регистрация причины обращения, подробности возникшей претензии Участника Платежной системы. По каждому обращению организуется анализ, основанный на опросе персонала, изучения системных журналов, определение условий недопущения таких ситуаций в дальнейшем.

6.5. Все решения по обращениям Участников Платежной Системы обязательно должны быть доведены Оператором до адресата с полным разъяснением изученных обстоятельств.

7 ПОРЯДОК ВЫХОДА УЧАСТНИКОВ ИЗ ПЛАТЕЖНОЙ СИСТЕМЫ

7.1. Порядок выхода из платежной системы при взаимодействии с Поставщиком товаров/услуг

7.1.1. Договор с Поставщиком товаров/услуг вступает в силу со дня его подписания Сторонами и действует до момента его расторжения по соглашению Сторон или в течение срока, определенного Договором с Поставщиком товаров/услуг,

7.1.2. Договор с Поставщиком товаров/услуг может быть расторгнут в одностороннем порядке, на основании заявления (по инициативе) Оператора, в следующих случаях:
- Нарушения Поставщиком товаров/услуг условий заключенного договора и/или настоящих Правил;
- Принятия соответствующим уполномоченным государственным органом нормативного правового акта, запрещающего или ограничивающего предпринимательскую деятельность Поставщиков случае, когда форс-мажорные обстоятельства длятся более шестидесяти (60) календарных дней, если иное не предусмотрено Договором с Поставщиком товаров/услуг;
- В случае, когда форс-мажорные обстоятельства длятся более 60 (шестидесяти) календарных дней.

7.1.3. Договор с Поставщиком товаров/услуг может быть расторгнут в одностороннем порядке, на основании заявления (по инициативе) Поставщика товаров/услуг, в следующих случаях:
- Нарушения Оператором условий заключенного договора и/или настоящих Правил;
- В случае, когда форс-мажорные обстоятельства длятся более шестидесяти (60) календарных дней, если иное не предусмотрено Договором с Поставщиком товаров/услуг;

7.1.4. В случае расторжения Договора с Поставщиком товаров/услуг денежные обязательства Сторон, а также обязательства, определяющие ответственность за нарушение настоящих Правил или Договора с Поставщиком товаров/услуг, сохраняются до момента их исполнения;

7.2. Порядок выхода из платежной системы при взаимодействии с Агентом/ Участником

7.2.1. Договор с Агентом/ Участником вступает в силу со дня его подписания Сторонами и действует до момента его расторжения по соглашению Сторон или в течение срока, определенного Договором, при условии, что срок Договора с Агентом/ Участником не превышает срока действия настоящих Правил;

7.2.2. Договор с Агентом/ Участником может быть расторгнут в одностороннем порядке, на основании заявления (по инициативе) Оператора, в следующих случаях:
- Нарушения Агентом/ Участником условий договора;

7.2.3. Договор с Оператором может быть расторгнут в одностороннем порядке, на основании заявления (по инициативе) Агента/ Участника в следующих случаях:
- Нарушения Оператором условий заключенного договора;
- В случае, когда форс-мажорные обстоятельства длятся более шестидесяти (60) календарных дней, если иное не предусмотрено Договором с Агентом/ Участником;

7.2.4. В случае одностороннего расторжения Договора с Оператором, Сторона-инициатор обязана уведомить другую Сторону в письменной форме не позднее, чем за тридцать (30) календарных дней до намеченной даты расторжения Договора с Оператором, если иное не предусмотрено Договором с Оператором;

7.2.5. В случае расторжения Договора с Агентом/ Участником денежные обязательства Сторон, а также обязательства, определяющие ответственность за нарушение настоящих Правил или Договора, сохраняются до момента их исполнения;

8. ОБЕСПЕЧЕНИЕ ФИЗИЧЕСКОЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

8.1. Оператор в целях обеспечения физической и информационной безопасности Платежной системы принимает доступные меры по обеспечению следующих требований:

1) Ограничивает доступ к центру обработки и каналам связи, используемым для передачи информации по платежам;
2) Реализует механизмы защиты данных как во время их хранения, так и в процессе передачи;
3) Обеспечивает адекватное резервирование всех данных (резервирование в реальном времени в отношении всей информации или ключевой информации);
4) Обеспечивает защиту системы от вредоносного программного обеспечения, регулярное обновление антивирусного программного обеспечения.
5) Обеспечивает целостность и подлинность данных при их передаче по каналам связи с места ее инициирования до процессингового центра и обратно;
6) Поддерживает работоспособность информационных систем, имеющих отношение к информационной безопасности;
7) Обеспечивает своевременное переключение/восстановление/разворачивание функционирования системы на резервном аппаратно-программном комплексе при возникновении нештатной ситуации;
8) Реализует механизмы проверки личности и правомочности лиц, производящих, обрабатывающих и получающих платежи;
9) Реализует механизмы минимизации ошибок ввода данных, контроль ввода данных, исключающий или снижающий возможность ошибки;
10) Проводит тщательное тестирование всего оборудования и программного обеспечения систем.
11) Обеспечивает защиту данных и оборудования при сбоях автоматизированной системы, нештатных ситуациях или в случае несанкционированного доступа к данным;
12) Проводит мониторинг и контролирует работоспособность объектов, подключенных к процессинговому центру, сеансов доступа к информационным ресурсам системы
13) Обеспечивает резервирование оборудования и системы связи;
14) Обеспечивает конфиденциальность информации Платежной системы;
15) Обеспечение физическую безопасность помещений и оборудования в соответствии с требованиями законодательства Кыргызской Республики;

9. МЕРЫ ЗАЩИТЫ ОТ МОШЕННИЧЕСТВА И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Оператор принимает в целях защиты от мошенничества и несанкционированного доступа к Платежной системы принимает доступные меры по обеспечению следующих требований:

9.1. Ограничивает доступ к центру обработки платежей и каналам связи, используемым для передачи информации по платежам;
9.2. Обеспечивает шифрование каналов передачи данных;
9.3. Реализует механизмы проверки личности и правомочности лиц, проводящих, обрабатывающих и получающих платежи;
9.4. Обеспечивает разделение обязанностей при выполнении действий по изменению данных информационной системы и подтверждения (санкционирования) их при необходимости не менее 2 (двумя) сотрудниками;
9.5. Обеспечивает авторизацию и аутентификацию участников и персонала системы.

9.6. Устанавливает каждому пользователю соответствующего права доступа, необходимого для выполнения им возложенных должностных обязанностей и обеспечения взаимозаменяемости;
9.7. Обеспечивает контроль за нарушениями режима информационной безопасности;
9.8. Обеспечивает физическую защиту информационных систем;
9.9. Обеспечивает криптографическую защиту данных;
9.10. Обеспечивает меры противопожарной безопасности;
9.11. Обеспечивает протоколирование и проверку технического состояния систем;
9.12. Обеспечивает защиту поддерживающей инфраструктуры и проводит обучение персонала;
9.13. Обеспечивает защиту от перехвата данных, защиту мобильных систем;
9.14. Использует антивирусную защиту на всех рабочих местах и серверах системы, если иное не предусмотрено технологическим процессом.

10. КРИТЕРИИ БЕСПЕРЕБОЙНОГО ФУНКЦИОНИНИЯ ПЛАТЕЖНОЙ СИСТЕМЫ

10.1. Критерии бесперебойного функционирования системы (БФС):

- уровень бесперебойности операционной деятельности;
- уровень бесперебойности оказания услуг платежного Процессинга;
- уровень бесперебойности осуществления расчетов между участниками платежной системы.

10.2. Факторы, влияющие на БФС:

- финансовое состояние Участников Платежной Системы;
- предусмотренные в Системе возможные способы управления ликвидностью и обеспечения исполнения обязательств Участников Платежной Системы (в сочетании с требованиями, предъявляемыми к финансовому состоянию Участников Платежной Системы);
- зависимость от внешних Поставщиков услуг;
- надежность технической системы;
- технологическое обеспечение Поставщиков услуг Системы, Участников/Агентов;
- возможность выявления неурегулированных вопросов правового характера, касающихся взаимоотношений Участников Платежной Системы;
- возможность возникновения конфликта интересов Участников Платежной Системы при осуществлении ими деятельности, направленной на достижение собственных целей и целей, установленных в рамках Системы (в том числе по обеспечению БФС);
- рыночные и инфраструктурные факторы;
- иные внешние и внутренние факторы, в соответствии с особенностями функционирования Системы.

10.3. Стратегия обеспечения БФС строится на базе контроля следующих бизнес процессов:

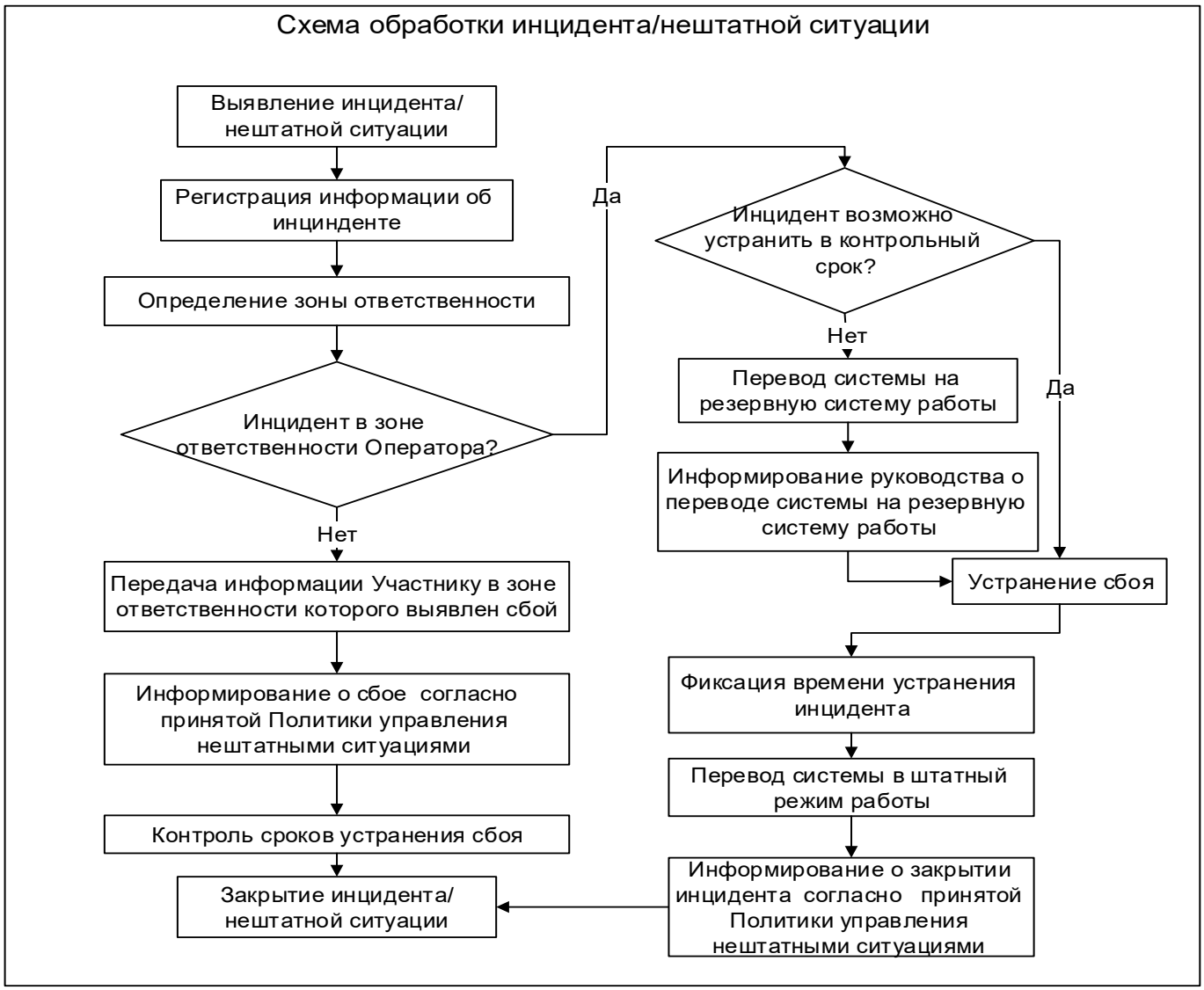
- оценка возможных рисков, присущих видам деятельности Оператора для обеспечения непрерывной деятельности Системы;
- контроля за соблюдением требований настоящих Правил, договорных обязательств, контроля за соблюдением порядка обеспечения БФС Участниками;
- проверка Участников на предмет соблюдения условий осуществления проведения Платежей, требований настоящих Правил;
- контроль за использованием наименования и товарных знаков Оператора исключительно в рамках заключенных договоров, соглашений и настоящих Правил;
- работы по уведомлению Участников о каких-либо отклонениях обеспечения функционирования Системы;

- оценка и мониторинг финансовой устойчивости Участников, факторов, несущих риски потери финансовой устойчивости Участников, в том числе потенциальных, способных привести к потере финансовой устойчивости Системы в будущем;
- проведение расследования событий, вызвавших операционные сбои, анализ их причин и последствий;
- анализ и оценка деятельности в соответствии требований законодательства КР, рекомендаций НБКР;
- обеспечения надежности, полноты и своевременности финансовой информации и отчетности, используемой для принятия решений, составления финансовой и регулятивной отчетности;
- наличие стабильного телекоммуникационного канала связи между Оператором и Участниками в рамках требований технологического взаимодействия;
- наличие бесперебойного электропитания на ключевых узлах Системы;
- поддержка бесперебойного функционирования программного комплекса управления терминальной сетью;
- поддержка бесперебойного функционирования SMS-шлюза;
- поддержка бесперебойного функционирования web-приложения, мобильного приложения, системы электронного кошелька;
- поддержка бесперебойного функционирования почтового сервиса;
- поддержка бесперебойного функционирования серверов Системы;
- обработка инцидентов платежной системы;
- обеспечение защиты информации от воздействия вредоносного кода;
- обеспечение внутреннего контроля по противодействию финансированию терроризма (экстремизма) и легализации (отмыванию) доходов, полученных преступным путем;
- обеспечение защиты информации при проведении платежных транзакций и взаимодействия с Участниками;
- выявление нештатных, чрезвычайных, нестандартных ситуаций и определение порядка взаимодействия Участников.

11. УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

При управлении инцидентами Участниками платежной системы должны учитываться, а Оператором обязательно исполняться следующие меры по выявлению возможных рисков и сложностей:

- Необходимость раннего обнаружения Инцидентов – организация мониторинга событий, а также обучение пользователей информированию об инцидентах
- Необходимость регистрации инцидентов
- Необходимость обеспечения высокой доступности к системе
- Нехватка ресурсов при решении инцидентов, перегруженность инцидентами и откладывание «на потом» — при неожиданном росте количества инцидентов для правильной регистрации может не оказаться достаточно времени.



Работа в процессе управления инцидентами строится по классической трехуровневой схеме:

Первый уровень - единая точка входа обращений.
Осуществляются регистрация и классификация заявок, определение их приоритета и ответственных за исполнение, отвечающих за решение типовых Инцидентов. .Этот уровень поддержки ведется в основном call-центром, которые обеспечены необходимыми документами и инструкциями, включая процесс взаимодействия со вторым уровнем.

Второй уровень
Инженеры поддержки — проводят техническую экспертизу и решают нетиповые инциденты, отвечают за обновление базы знаний о приложении, выявляют дефекты и передают их на третий уровень поддержки. Решение проблем передается на третий уровень, если причина связана с архитектурой системы или его программной реализацией.

Третий уровень
Специалисты по технической поддержке работы системы осуществляют анализ сложных инцидентов, не решенных на втором уровне, исправляют дефекты, тестируют предоставленные решения.

12. ПОРЯДОК ИНФОРМИРОВАНИЯ УЧАСТНИКОВ

Доведение до Участников системы информации о нарушениях и неисправностях в работе Платежной системы Оператора и возникших в связи с этим рисках осуществляется если возникший Инцидент влияет на бесперебойное функционирование платежной системы.

Подтверждение (или опровержение) Участником платежной системы (в зоне ответственности которого находятся заявленные нарушения и неисправности) факта нарушения (с указанием даты, времени возникновения, времени устранения, характера нарушений и неисправностей, причин их возникновения и принятых мерах по их устранению, результатах расследования указанных событий, анализа последствий), производится путем обращения к Стороне по телефонным каналам связи или по электронной почте с установленных адресов на установленный адрес. Оператор также использует любые дополнительные доступные способы коммуникации, включая информирование широкой общественности, для обеспечения максимального уровня осведомленности всех участников о возникшей нештатной ситуации и принятия эффективных мер ее решения.

Процедура информирования Национального банка КР, а также Участников платежной системы после устранения нештатной ситуации и восстановления штатного функционирования системы осуществляется в течение не более 8 часов, и в порядке, предусмотренном договорами сторон.

При возникновении Инцидента, который может негативно отразиться на бесперебойности Платежной системы. Участник платежной системы выявивший инцидент:

- уведомляет сторону или стороны, подвергающиеся риску,
- принимает меры по исполнению/завершению своих финансовых обязательств перед участниками платежной системы;
- принимает меры по обеспечению сохранности данных и восстановлению работоспособности платежной системы;
- обеспечивает для других Участников возможность выполнения своих обязательств.

Информирование Национального банка КР Оператором возникшем инциденте осуществляется, в случае неработоспособности платежной системы длятся более 2 часов.

Доведение до Участников платежной системы информации о нарушениях и неисправностях в работе Платежной системы и возникших в связи с этим рисках осуществляется, если уровни риска в результате нарушения относятся к категории «Средний» или «Высокий» и влияют на бесперебойное функционирование систем Участников.

При наступлении события, которое определяется уровнем риска как «Средний» либо «Высокий», в условиях, что выявленные нарушения работы влияют на бесперебойное функционирование Платежной системы в целом, Оператором осуществляется незамедлительное уведомление Управления платежных систем НБКР по телефонным каналам связи, по электронной почте и любому другому средству связи доставки сообщений адресату.

При выявлении фактов внешних угроз, преступлений, мошенничества в Платежной системе, которое может угрожать другим Участникам, незамедлительно производится уведомление Управления платежных систем НБКР по телефонным каналам связи, по электронной почте и любому другому средству связи доставки сообщений адресату.

13. Меры ПФТД/ЛПД

1. Применение программы внутреннего контроля

Оператор применяет правила внутреннего контроля в соответствии с законодательством Кыргызской Республики в сфере ПФТД/ЛПД для выполнения следующих основных обязанностей по ПФТД/ЛПД:

1) осуществление мер по выявлению, оценке, мониторингу, управлению, снижению и документированию рисков;

2) осуществление мер надлежащей проверки пользователей;

3) применение целевых финансовых санкций и приостановление операций (сделок);

4) применение мер в отношении высоко рискованных стран;

5) своевременное представление в орган финансовой разведки информации и документов, а также сообщений об операциях (сделках), подлежащих контролю и сообщению;

6) обеспечение хранения сведений и документов об операциях (сделках), а также информации, полученной по результатам надлежащей проверки пользователя;

7) обеспечение конфиденциальности сведений;

8) обеспечение выполнения иных обязанностей, предусмотренных в законодательстве К Кыргызской Республики в сфере ПФТД/ЛПД.

2. Использование перечней и списков

Оператор обеспечивает интеграцию Сводного санкционного перечня Кыргызской Республики, Сводного санкционного перечня Совета Безопасности ООН, Перечня лиц, групп, организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов, Перечня физических лиц, отбывших наказание за осуществление легализации (отмывания) преступных доходов, террористической или экстремистской деятельности, а также за финансирование данной деятельности в платежную систему в целях обеспечения онлайн мониторинга идентификационных сведения и их сверки.

3. Меры по обеспечению прозрачности бенефициарных владельцев

Все юридические лица - контрагенты Оператора, созданные и зарегистрированные в Кыргызской Республике, в том числе поставщики товаров и услуг, операторы платежных систем и платежные организации, Агенты/ Участники обязаны:

- формировать достоверную и обновленную информацию о физическом лице, которое в конечном итоге (через цепочку владения и контроля) прямо или косвенно (через третьих лиц) владеет правами собственности данного юридического лица или контролирует данное юридическое лицо (далее - бенефициарный владелец) на основе имеющейся и доступной информации, а также принять все доступные и возможные меры для установления своего бенефициарного владельца;

- Оператор хранит полученную информацию о бенефициарном владельце не менее пяти лет с даты ее формирования.

4. Применение риск-ориентированного подхода

Оператор применяет риск-ориентированный подход в своей деятельности, а именно:

1) оценивает и постоянно обновляет свои риски с учетом особенностей деятельности, результатов национальной оценки рисков и типичных критериев высоких и низких рисков;

2) в установленном порядке представляет информацию о выявленных рисках соответствующему проверяющему органу и органу финансовой разведки;

3) разрабатывает и применяет усиленную или упрощенную политику, а также меры контроля, процедуры по управлению и снижению рисков;

4) принимает усиленные или упрощенные меры надлежащей проверки пользователя с учетом результатов оценки рисков;

5) классифицирует Участников с учетом критериев риска.

5. Осуществление надлежащей проверки

Оператор применяет самостоятельно проверку, или полагается на результаты проверки другой стороны, в соответствии с законодательством, в отношении всех своих пользователей Участников следующие меры надлежащей проверки:
1) идентификация и верификация Участников;
2) получение информации о цели и предполагаемом характере деловых отношений Участника;
3) идентификация бенефициарного владельца и принятие доступных мер для верификации бенефициарного владельца;
4) документально фиксирует сведения, полученные в результате идентификации и верификации Участника и бенефициарного владельца;
5) хранит и обновляет информацию и документы о деятельности Участника и его финансовом положении, а также сведения и документы, полученные в результате надлежащей проверки клиента;
6) проводит на постоянной основе надлежащую проверку Участника (на протяжении всего периода деловых отношений с пользователем и анализ соответствия операций (платежей), проводимых пользователем и в пользу пользователя, с имеющейся информацией о содержании его деятельности, финансовом положении и об источнике средств, а также о характере рисков финансирования террористической деятельности и легализации (отмывания) преступных доходов.
Также Оператор вправе применять следующие дополнительные меры надлежащей проверки пользователя в отношении публичных должностных лиц, в том числе в отношении членов семьи и близких лиц (близкие родственники, деловые партнеры и официальные представители):
1) использует систему управления рисками для определения того, является ли Участник или бенефициарный владелец публичным должностным лицом;
2) получает письменное разрешение руководителя организации для установления или продолжения (для существующих Участников) деловых отношений с публичным должностным лицом;
3) устанавливает источник происхождения денежных средств или иного имущества публичного должностного лица;
4) проводит постоянный и углубленный мониторинг деловых отношений, в том числе операций (сделок), осуществляемых публичным должностным лицом, в порядке, установленном для пользователя высокого риска.
Оператор проводит надлежащую проверку в любом из следующих случаев:
1) при установлении деловых отношений;
2) при совершении разовой операции (платежа), в том числе перевода, или нескольких взаимосвязанных разовых операций (платежей) на сумму, равную или превышающую 70000 сомов.
3) при совершении разового электронного денежного перевода на сумму, равную или превышающую 70000 сомов или эквивалента в иностранной валюте;
4) при наличии подозрения в осуществлении финансирования террористической деятельности и легализации (отмывания) преступных доходов, независимо от статуса клиента (постоянный или разовый) или любых исключений либо независимо от пороговой суммы операции (сделки);
5) при выявлении фактов недостоверности или недостаточности ранее полученных сведений о клиенте.
При проведении трансграничных платежей:
1) Оператор и его агенты обязаны принять доступные меры по обеспечению наличия следующих сведений:
- фамилия, имя и отчество отправителя - физического лица;
- номер счета отправителя, если при осуществлении платежа использовался счет;
- паспортные данные отправителя - физического лица;
- идентификационный номер пользователя;

при трансграничных переводах (на персональный лицевой счет, электронный кошелек или банковский счет):

- фамилия, имя и отчество получателя - физического лица;
- номер счета получателя, если при осуществлении платежа используется счет. При отсутствии счета Оператор обеспечивает присвоение уникального кода транзакции.

2) Оператор должен проверять отправителя и получателя платежа на наличие или отсутствие в Санкционных перечнях и Перечне лиц, групп и организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов;

3) Оператор имеет право замораживать или приостанавливать платеж и в течение трех часов сообщать об этом в орган финансовой разведки - в случае наличия отправителя и (или) получателя денежного перевода в Санкционных перечнях и Перечне лиц, групп и организаций, в отношении которых имеются сведения об их участии в легализации (отмывании) преступных доходов.

6. Хранение сведений и документов

Оператор хранит следующие сведения и документы:

1) сведения, деловая переписка и копии документов, в том числе подлинники анкет пользователя и бенефициарного владельца, полученные в результате надлежащей проверки пользователя, - не менее пяти лет после прекращения деловых отношений с пользователем или проведения последней операции с пользователем;

2) сведения и документы обо всех проведенных операциях (платежах) - не менее пяти лет после завершения операции (платежа);

3) заключения или справки по анализу проведенных операций (платежей) - не менее пяти лет после завершения операции (платежа);

4) сведения и документы, предусмотренные законодательством Кыргызской Республики в сфере противодействия финансированию террористической деятельности и легализации (отмыванию) преступных доходов, - не менее пяти лет после прекращения деловых отношений с клиентом или проведения последней операции (платежа) с пользователем.

7. Предоставление сообщений об операциях и сделках

Оператор направляет в орган финансовой разведки сообщения о следующих операциях (платежах), подлежащих контролю и сообщению, в виде электронного документа (далее - электронное сообщение), путем заполнения соответствующей типовой формы:

1) сообщение о подозрительной операции (платеже) - в течение пяти часов с момента признания в установленном порядке операции (платежа) подозрительной;

2) сообщение об операции (платеже) с физическими или юридическими лицами из высоко рискованных стран (перечень размещается на официальном сайте ответственного государственного органа) - в течение двух рабочих дней со дня совершения такой операции (платежа);

3) сообщение об операциях (платежах), совершенных физическим лицом, отбывшим наказание за осуществление легализации (отмывания) преступных доходов, террористической или экстремистской деятельности, а также за финансирование такой деятельности, - в течение двух рабочих дней со дня совершения таких операций (платежа);

4) сообщение об операции (платеже) с наличными денежными средствами - в течение трех рабочих дней со дня совершения такой операции (платежа).

14. Лимиты, установленные в Системе

14.1 Лимиты, установленные в системе соответствуют действующему законодательству в отношении операторов платежной системы, платежных организаций (в том числе платежей МПА), операторов электронных денег.

14.2 Помимо лимитов, установленных законодательством Оператор вправе устанавливать собственные лимиты, установленные Оператором исходя из текущей конъюнктуры рынка и анализа оценки рисков Платежной системы в соответствии с политикой управления рисками.

15. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ

15.1. В правилах платежной системы запрещается установление требований к Участникам платежной системы о неучастии в других платежных системах (условия об исключительном участии).

15.2. Правила и процедуры системы Оператора должны давать Участникам четкое представление о влиянии системы на каждый из финансовых рисков, которые они несут в силу участия в системе, объяснять юридическую основу и роли сторон-участников, время и принципы управления рисками системы.

15.3. Правила и процедуры системы Оператора должны соответствовать требованиям нормативных правовых актов Национального банка по управлению рисками, регулярно пересматриваться и обновляться в случае необходимости, но не реже 1 (одного) раза в 3 (три) года.

16. ПРИЛОЖЕНИЯ

16.1. Список приложений:

Неотъемлемой частью Правил являются следующие Приложения:

1) Приложение № 1 - Система управления рисками, используемая модель управления рисками, перечень мероприятий и способов управления рисками
2) Приложение № 2 - Порядок действия Участников Платежной системы при возникновении нештатных ситуаций в Системе
3) Приложение № 3 - Архитектура Системы приема платежей, схема ее работы.
4) Приложение № 5 - Порядок проведения процессинга
5) Приложение № 6 – Тарифная политика
6) Приложение №7 – Лимиты, установленные в системе.

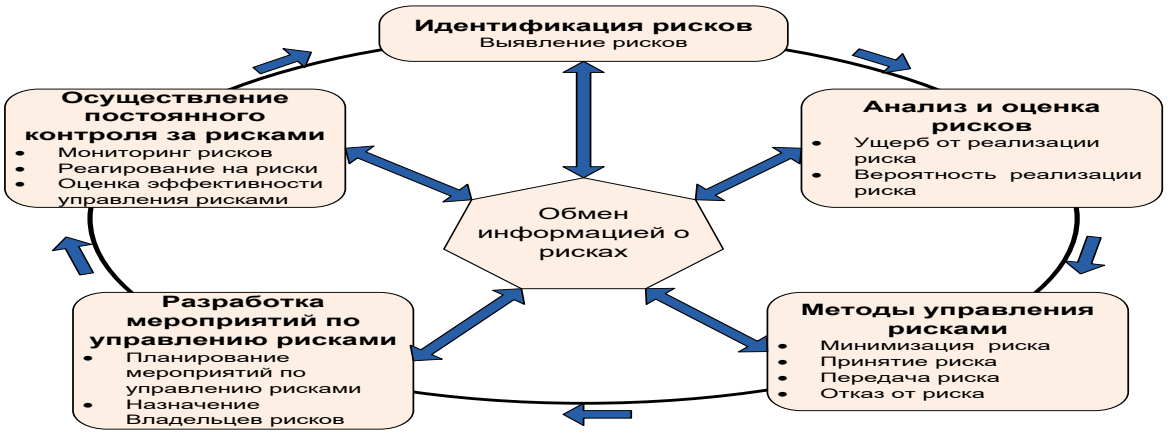
Приложение № 1
к Правилам Платежной Системы

Система управления рисками Оператора.

Достижение целей управления рисками предполагает выполнение следующих задач:

- прогнозирование наступления неблагоприятных событий, при реализации которых может быть нарушено бесперебойное функционирование платежной системы;
- содействие устойчивой работе платежной системы;
- предупреждение и предотвращение возникновения рисков;
- идентификация и выявление рисков и определение причин их возникновения;
- определение приоритетности рисков;
- сдерживание рисков;
- оценка уровня и степени влияния рисков;
- мониторинг и анализ рисков на постоянной основе;
- организация процесса своевременного устранения последствий возникновения рисков и создание механизмов восстановления работоспособности платежных систем в случае ее нарушения;
- определение способов достижения и поддержания приемлемого уровня рисков в платежной системе;
- обеспечение информационного взаимодействия участников платежной системы в целях реализации мероприятий, направленных на снижение выявленных рисков;
- выработка и осуществление мер, направленных на противодействие факторам рисков, и принятие управленческих решений по регулированию платежных систем;
- оперативное реагирование процесса управления рисками к изменяющимся условиям рынка услуг платежной инфраструктуры.

Принятая модель управления рисками



Основной целью по управлению рисками в Платежной системе является выработка и осуществление мер по ограничению, минимизации риска и оперативному принятию управленческих решений по регулированию Платежной системой.

Функционирование Платежной системы может быть нарушено в результате реализации рисков, в том числе возникновения неблагоприятных событий, связанных с действием или бездействием одного, нескольких или большинства Участников платежной системы и (или) недостатками в организации и (или) обеспечении деятельности Платежной системы.

Системный риск.

Системный риск - риск наступления неблагоприятного события, при котором неспособность одного из участников платежной системы выполнить свои обязательства по платежам повлечет для других участников невыполнение своих обязательств при наступлении срока платежа. Такое невыполнение обязательств может поставить под угрозу стабильность всей платежной системы (эффект "домино").

Факторы системного риска делятся:

Внутренние факторы риска.

Антропогенный фактор. Возникновение угрозы безопасности информации в результате отсутствия профессиональных навыков, недостаточной подготовки, халатности, ненадлежащего исполнения обязанностей или злого умысла персонала, эксплуатирующего информационно-телекоммуникационные средства, системы и сети, разработчиков программного обеспечения и пользователей, имеющих допуск к информации на законном основании. Нарушение правил эксплуатации IT оборудования, их систем и сетей лицами, ответственными за эту работу;
Системный фактор. Возникновение угрозы целостности информации и (или) функционированию информационно-телекоммуникационных средств, систем и сетей в результате ошибок в их проектировании и разработке или возникновения внутрисистемных сбоев (фатальных ошибок) при их эксплуатации, в том числе, из-за несовершенства или конфликтов программного обеспечения, или неисправности оборудования.

Внешние факторы риска.

Фактор кибербезопасности. Целенаправленное внешнее воздействие на информационные ресурсы и информационно-телекоммуникационные средства, системы и сети («атаки», вторжения) с целью уничтожения, блокирования или копирования информации, разработка и внедрение вредоносных программ (вирусов, симуляторов, «троянских» программ, клавиатурных перехватчиков и др.) внедрение специальных технических средств для негласного получения информации;
Техногенный фактор. Совокупность угроз искусственного характера, вызванных результатами человеческой деятельности (цивилизации) - пожары, взрывы, затопления, радиационные и химические заражения, энергетические аварии, разрушение коммуникаций, в том числе, в результате террористических актов, диверсий, массовых беспорядков и ведения боевых действий.
Природный фактор. Совокупность угроз природного характера, являющихся следствием воздействия естественной непреодолимой силы (стихии) - землетрясения, наводнения, метеорологические катаклизмы и т.п., приводящие к устойчивому нарушению функционирования информационных и телекоммуникационных ресурсов, вплоть до их утраты или физического уничтожения. Вероятность определяется спецификой территории, на которой дислоцируется защищаемый объект: многолетними метеорологическими наблюдениями, геотектоническими данными и другими критериями.

Механизмы снижения влияния системного риска.

- Постоянный мониторинг значительных системных событий, которые неблагоприятно воздействуют на системно значимых участников платежной системы, рынки и соответствующую инфраструктуру
- Обеспечение реализации механизмов гарантирующих проведение платежей;
- Усиленный контроль за платежными и расчетными системами;
- Приоритизация видов платежей по их типу: социально значимые, бюджетообразующие и пр.

Операционный риск.

Операционный риск - риск, возникающий вследствие нарушения функционирования аппаратно-программного комплекса и коммуникационных каналов связи, ненадлежащего действия персонала и должностных лиц участников платежной системы, а также воздействия внешних факторов, которые приводят к невозможности проведения платежей и расчетов, нарушению правил платежной системы, а также информационной безопасности, либо невозможности функционирования платежной системы в целом.
Локализацией (местом проявления) операционного риска являются структурные подразделения и аппаратно-программные комплексы Участников платежной системы, в разрезе которых осуществляется контроль проявления операционного риска.

Формой реализации операционного риска являются нарушения функционирования Платежной системы в результате нарушения работоспособности аппаратно-программных комплексов Участников платежной системы, выполнения недопустимых операций или ошибочного выполнения операций в Платежной системе.

Механизмы снижения влияния операционного риска

По обеспечению работоспособности аппаратно-программных комплексов:
– разработка технических требований на создание, внедрение и эксплуатацию аппаратно-программных комплексов с учетом требований к показателям бесперебойности;
– тестирование аппаратно-программных комплексов перед их внедрением;
– регулярный мониторинг системного, прикладного программного обеспечения и доступа к информационным ресурсам;
– обеспечение целостности информационных активов путём применения: средств идентификации и аутентификации; процедур протоколирования и аудита; криптографической защиты информации; резервного копирования и архивирования информационных ресурсов;
– обеспечение резервирования критичных информационных активов;
– разработка, поддержание в актуальном состоянии планов обеспечения непрерывности деятельности и восстановления деятельности после сбоев;
– проведение регулярной оценки качества и надежности функционирования информационных систем, операционных и технологических средств, соответствие их отраслевым нормативным актам.
– дублирование аппаратного и программного обеспечения в основном узле;
– дублирование в резервном центре аппаратно-программного комплекса основного узла;
– наличие удаленного резервного центра;
– дублирование каналов связи для обеспечения непрерывной связи между основным узлом и автоматизированными рабочими местами участников;
– организация бесперебойного электроснабжения основного и резервного узлов;

– обеспечение средств авторизации и аутентификации участников и персонала системы, шифрование каналов передачи данных для защиты от несанкционированного доступа;
– обеспечение возможности применения электронной цифровой подписи для обеспечения достоверности и целостности передаваемой информации;
– обеспечение резервного копирования всех операций, проводимых в системе для хранения и восстановления данных в случае возникновения опасности потерь или их дублирования;
– наличие системы безопасности (информационные, технические и физические);

По персоналу:
– наличие квалифицированного персонала системы (основной и дублирующий состав) и обеспечение регулярного обучения;
– ограничение функций и полномочий сотрудников;
– обучение персонала новым информационным технологиям, повышение его квалификации, периодическое тестирование.

Кредитный риск и риск ликвидности

Кредитный риск - риск, возникающий вследствие неспособности участника платежной системы исполнить свои финансовые обязательства по оплате оказанных услуг платежной инфраструктуры перед другими участниками при наступлении срока платежа или в любое последующее время. Кредитный риск создает угрозу финансовой устойчивости участников платежной системы, что может повлиять на бесперебойность функционирования платежной системы.
Риск ликвидности - риск, возникающий вследствие неспособности участника платежной системы в связи с недостатком или отсутствием денежных средств обеспечить исполнение своих обязательств в полном объеме в срок исполнения платежа. Наступление данного вида риска связано с несбалансированностью финансовых активов и финансовых обязательств участника платежной системы.

Механизмы снижения влияния кредитного риска и риска ликвидности

– мониторинг в режиме реального времени достаточности средств участников для исполнения своих обязательств по проведению платежей;
– обеспечение возможности резервирования средств для обеспечения гарантированного проведения расчета;
– обработка платежей в соответствии с установленными приоритетами;
управление участниками очередью своих платежей (изменение приоритетов платежей, отзыв платежей из очереди платежей и т.д.);
- обеспечение двойного ввода ключевых полей при подготовке платежных документов в ручном режиме; - ведение архивов всех отправленных и поступивших электронных сообщений для обеспечения сохранности электронных документов в системе; осуществление регулярного контроля соблюдения участниками правил функционирования системы.
– периодическая оценка платежеспособности участников платежной системы, а также исключение участников платежной системы не соответствующих требованиям законодательства Кыргызской Республики.

Правовой риск

Правовой риск - риск, возникающий вследствие несоблюдения требований законодательства

Кыргызской Республики, условий договоров и соглашений, внутренних документов участников платежных систем, определяющих нормы и правила функционирования платежных систем.
Источником правового риска является несоблюдение Участниками платежной системы требований законодательства, нормативных актов и заключенных договоров, внутренних документов, регламентирующих их деятельность, а также наличие недостатков внутренних документов, несоответствие деятельности Общества требованиям законодательства.
Формой реализации правового риска являются претензии правового характера к Участникам платежной системы со стороны других Участников платежной системы, со стороны государственных органов, со стороны клиентов Участников платежной системы, надзорного органа.

Локализацией (местом проявления) правового риска являются:
– Участники платежной системы, которым могут быть предъявлены претензии правового характера, связанные с несоблюдением требований законодательства, нормативных актов и заключенных договоров;
– внутренние документы Участников платежной системы и договоры, содержание которых подлежит постоянному контролю на соответствие законодательству и нормативным актам, с учетом вносимых в них изменений.

Механизмы снижения влияния правового риска

В целях минимизации юридических/правовых рисков в системе принимаются меры по устранению правовой неопределенности в отношениях с участниками платежных систем, осуществляется контроль за соблюдением участниками платежных систем законодательства Кыргызской Республики, контроль за соответствием условий договоров и соглашений, внутренних документов, а также норм и правил работы систем требованиям законодательства КР.

Риск мошенничества.

Возникает вследствие неправомерных действий работников и должностных лиц участника платежных систем, заключающихся в злоупотреблении служебным положением, несанкционированном использовании служебной информации, хищении денежных средств, преднамеренном сокрытии фактов совершения операций в рамках платежной системы, а также противоправных действий сторонних лиц по отношению к платежной системе, таких как хищение персональных данных, получение конфиденциальной информации, проникновение в базу данных с целью хищения денежных средств и т.д.

Механизмы снижения влияния риска мошенничества.

В целях предотвращения проведения несанкционированных операций в платежной системе применяется механизм проверки личности и правомочности лиц, проводящих, обрабатывающих и получающих платежи, обеспечиваться конфиденциальность информации, а также ограничиваться доступ к центрам обработки платежей и каналам связи, используемым для передачи информации по платежам. Обеспечение физической безопасности помещений и оборудования, а также защиты данных как во время их хранения, так и в процессе передачи.

Риск хакерской атаки.

Риск, возникающий вследствие воздействия на информационные ресурсы и информационно-телекоммуникационные средства платежной системы путем несанкционированного входа в

информационные системы, внедрения специальных технических средств, заражения компьютерными вирусами и другими вредоносными программами с целью хищения денежных средств, получения персональной информации пользователей (пароли, ПИН-коды, номера банковских карт, аналог собственноручной подписи, персональные данные пользователей), уничтожения и нарушения целостности баз данных, блокирования и вывода из строя информационных компьютерных систем.

Механизмы снижения риска хакерской атаки.
Система управления информационной безопасностью представляет собой набор взаимосвязанных стратегических и операционных компонент для создания надежной программы по безопасности. Каждый компонент – это набор процессов и практик, работающие вместе и направленные на один аспект безопасности компании. Компоненты направлены как на физическую, так и на электронную безопасность. Нормы регламентирующие процессы информационной безопасности приведены в политике по информационной безопасности и положении по нештатным ситуациям.

Риск потери репутации.

Риск, возникающий вследствие формирования в обществе негативного представления о стабильности платежной системы, отрицательной оценки качества предоставляемых услуг в платежной системе, в том числе вследствие распространения ложной информации, ведущей к утрате доверия к платежной системе или участникам платежной системы.

Механизмы снижения риска потери репутации.

- принятие своевременных мер по устранению нарушений в деятельности Общества;
- содействие в соблюдение принципов профессиональной этики;
- при принятие управленческих решений учитывается взаимосвязь различных рисков, их возможность дополнять, усиливать или компенсировать друг друга;
- проведение периодических тренингов сотрудников;
- соблюдение принципа "Знай своего служащего";
- обеспечение идентификации контрагентов Общества.

Приложение № 2
к Правилам Платежной Системы

Порядок действий Участников Платежной Системы при возникновении нештатных ситуаций и системного риска в Системе.

При возникновении наиболее распространенных нештатных ситуаций:
Сбой программного обеспечения– Ответственное лицо совместно с техническими службами выясняет причину сбоя ПО. Если исправить ошибку своими силами не удалось, привлекают разработчиков.
Сбой в локальной вычислительной сети (ЛВС). Ответственное лицо по информационной безопасности организует анализ на наличие потерь и (или) разрушения данных и сетевого оборудования. В случае необходимости, производится восстановление ПО, замена оборудования из резерва, а также данные из последней резервной копии
Выход из строя сервера. Сотрудник, ответственный за эксплуатацию сервера проводит меры по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы компании. При необходимости производятся работы по восстановлению ПО и данных из резервных копий.
Потеря данных. При обнаружении потери данных ответственное лицо информационной безопасности (системный администратор) совместно с Техническим Директором, проводят мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность, и работоспособность оборудования и др.). При необходимости, производится восстановление ПО и данных из резервных копий.
Обнаружен вирус. При обнаружении вируса производится локализация вируса с целью предотвращения его дальнейшего распространения, для чего следует физически отсоединить «заражённый» компьютер от ЛВС и провести анализ состояния компьютера. Анализ проводится компетентным в этой области Результатом анализа может быть попытка сохранения (спасения данных), так как после перезагрузки ПЭВМ данные могут быть уже потеряны. После успешной ликвидации вируса, сохранённые данные также необходимо подвергнуть проверке на наличие вируса. При обнаружении вируса следует руководствоваться инструкцией по эксплуатации применяемого антивирусного ПО. После ликвидации вируса необходимо провести внеочередную антивирусную проверку на всех ПЭВМ компании с применением обновлённых антивирусных баз. При необходимости производится восстановление ПО и данных из резервных копий с составлением акта. Проводится служебное расследование по факту появления вируса в ПЭВМ (ЛВС).

Обнаружена утечка информации (дырка в системе защиты). При обнаружении утечки информации ставится в известность ответственное лицо по информационной безопасности и Технический Директор. Проводится служебное расследование. Если утечка информации произошла по техническим причинам, проводится анализ защищённости системы и, если необходимо, принимаются меры по устранению уязвимостей и предотвращению их возникновения.
Взлом системы (Web-сервера, сервера, файл-сервера и др.) или несанкционированный доступ (НСД). При обнаружении взлома сервера ставится в известность ответственное лицо информационной безопасности и Технический Директор. Проводится, по возможности, временное отключение сервера от сети для проверки на вирусы и троянские закладки. Возможен временный переход на резервный сервер. Учитывая, что программные закладки могут быть не обнаружены антивирусным ПО, следует особенно тщательно проверить целостность исполняемых файлов в соответствии с хэш-функциями эталонного программного обеспечения, а также проанализировать состояние файлов - скриптов и журналы сервера. Необходимо сменить все пароли, которые имели отношение к данному серверу. В случае необходимости производится восстановление ПО и данных из эталонного архива и резервных копий с составлением акта. По результатам анализа ситуации следует проверить вероятность

проникновения несанкционированных программ в ЛВС компании, после чего провести аналогичные работы по проверке и восстановлению ПО и данных на других ЭВМ компании. По факту взлома сервера проводится служебное расследование.

Попытка несанкционированного доступа (НСД). При попытке НСД проводится анализ ситуации на основе информации журналов регистрации попыток НСД и предыдущих попыток НСД. По результатам анализа, в случае необходимости, принимаются меры по предотвращению НСД, если есть реальная угроза НСД. Так же рекомендуется провести внеплановую смену паролей. В случае появления обновлений ПО, устраняющих уязвимости системы безопасности, следует применить такие обновления.

Компрометация ключей. При компрометации ключей следует руководствоваться инструкцией по эксплуатации применяемого ПО криптозащиты.

Компрометация пароля. При компрометаций пароля необходимо немедленно сменить пароль, проанализировать ситуацию на наличие последствий компрометации и принять необходимые меры по минимизации возможного (или нанесённого) ущерба (блокирование счетов и т.д.). При необходимости, проводится служебное расследование.

Физическое повреждение ЛВС или ПЭВМ. Ставится в известность ответственное лицо по информационной безопасности. Проводится анализ на утечку или повреждение информации. Определяется причина повреждения ЛВС или ПЭВМ и возможные угрозы безопасности информации. В случае возникновения подозрения на целенаправленный вывод оборудования из строя проводится служебное расследование. Проводится проверка ПО на наличие вредоносных программ-закладок, целостность ПО и данных. Проводится анализ электронных журналов. При необходимости проводятся меры по восстановлению ПО и данных из резервных копий с составлением акта.

Стихийное бедствие. При возникновении стихийных бедствий следует руководствоваться соответствующими документами Оператора.

Порядок и сроки информирования руководства и персонала системы о возникновении нештатной ситуации. При возникновении нештатной ситуации специалист по сопровождению системы в течение 30 минут информирует руководство и персонал системы о возникновении нештатной ситуации путем отправки сообщения по электронной почте и СМС на мобильные телефоны.

Регистрация факта возникновения нештатной ситуации. При возникновении нештатной ситуации специалист по сопровождению системы регистрирует факт возникновения нештатной ситуации (дату, время, описание события) в специальном журнале.

Порядок действий, если проблемы не были решены на уровне ответственных исполнителей персонала системы за предусмотренное процедурами время. Если проблемы не были решены на уровне ответственных исполнителей персонала системы за предусмотренное процедурами время - специалист по сопровождению системы ставит в известность Технического директора для принятия решения по дальнейшим действиям

Порядок информирования клиентов о крупном инциденте. В случае крупного инцидента Директор по проектам совместно с Председателем правления принимают решение о способе коммуникации и в случае необходимости информируют клиентов и общественность о произошедшем исходя из оценки величины инцидента.

Порядок и сроки информирования руководства и персонала системы после устранения нештатной ситуации и восстановления штатного функционирования системы. После восстановления штатного функционирования системы специалист по сопровождению системы в течение 30 минут информирует руководство и персонал системы о восстановлении штатного функционирования системы путем отправки сообщения по электронной почте и СМС на мобильные телефоны, регистрирует в специальном журнале дату, время, причину возникновения нештатной ситуации, содержание принятых мер по ее устранению с указанием ответственных исполнителей. В течение 2 рабочих дней Технический директор готовит акт и экспертное заключение по нештатной ситуации.

В целях превентивных мер по снижению риска возникновения несанкционированных операций в платежной системе – противоправные преднамеренные деяния (действия, бездействия, злоупотребление доверием) персонала оператора/участника системы или третьей стороны, направленные на несанкционированный доступ и использование информации, относящейся к банковской тайне, для получения/перевода денежных средств с /электронных кошельков участников системы и/или их клиентов.

Оператор устанавливает политику информационной безопасности (в том числе и информационных ресурсов системы) от несанкционированного доступа/операций, злоупотребления или мошеннического изменения (вставки, удаления, искажения, замены), или раскрытия данных/информации и проводит комплекс мер по обеспечению безопасности системы:

- имеет четко регламентированные задачи, требования по обеспечению конфиденциальности и доступу к информации, адекватности внутреннего контроля, а также критерии разграничения ответственности соответствующих лиц при осуществлении контроля;

- обеспечивает своевременное реагирование на возникновение подозрительной активности/операций в системе или попыток несанкционированного доступа/операций и порядок взаимодействия с правоохранительными органами Кыргызской Республики;

- незамедлительно (в тот же день, когда об этом событии стало известно) информирует Национальный банк в электронной форме о фактах внешних угроз, несанкционированного доступа/операций, злоупотребления, грабежа, нестабильной ситуации и т.д. В случае, если событие носит системный характер и может угрожать другим участникам финансовой системы Кыргызской Республики,

- предусматривает порядок подключения и использования ресурсов сети интернет,

- использует антивирусную защиту на всех рабочих местах и серверах системы;

- проводит разработку новых методов борьбы с несанкционированным доступом/операциями/мошенничеством;

- проводит регулярное обучение сотрудников по безопасности и персонала системы механизмам предотвращения мошенничества и несанкционированного доступа.

Процедура информирования Национальный банк, а также Участников платежной системы после устранения нештатной ситуации и восстановления штатного функционирования системы осуществляется в течение не более 8 часов, и в порядке, предусмотренном договорами сторон.

При возникновении инцидента, который может негативно отразиться на бесперебойности Участников:

- уведомляет сторону или стороны, подвергающиеся риску, агентов/поставщиков товаров/услуг;
- принимает меры по исполнению/завершению своих финансовых обязательств перед пользователями услуг (клиентами)/поставщиками товаров/услуг и участниками платежной системы;
- принимает меры по обеспечению сохранности данных и восстановлению работоспособности платежной системы;
- обеспечивает для других Участников возможность выполнения своих обязательств.

Информирование Национального банка КР о возникшем Инциденте осуществляется Оператором, в случае возникновения сбоев в работе платежной системы длящихся более 2 часов.

Доведение до Участников платежной системы информации о нарушениях и неисправностях в работе Платежной системы и возникших в связи с этим рисках осуществляется, если уровни риска в

результате нарушения относятся к категории «Средний» или «Высокий» и влияют на бесперебойное функционирование систем Участников.

При наступлении события, которое определяется уровнем риска как «Средний» либо «Высокий», в условиях, что выявленные нарушения работы влияют на бесперебойное функционирование Платежной системы в целом, осуществляется незамедлительное уведомление Управления платежных систем НБКР по телефонным каналам связи, по электронной почте и любому другому средству связи доставки сообщений адресату.

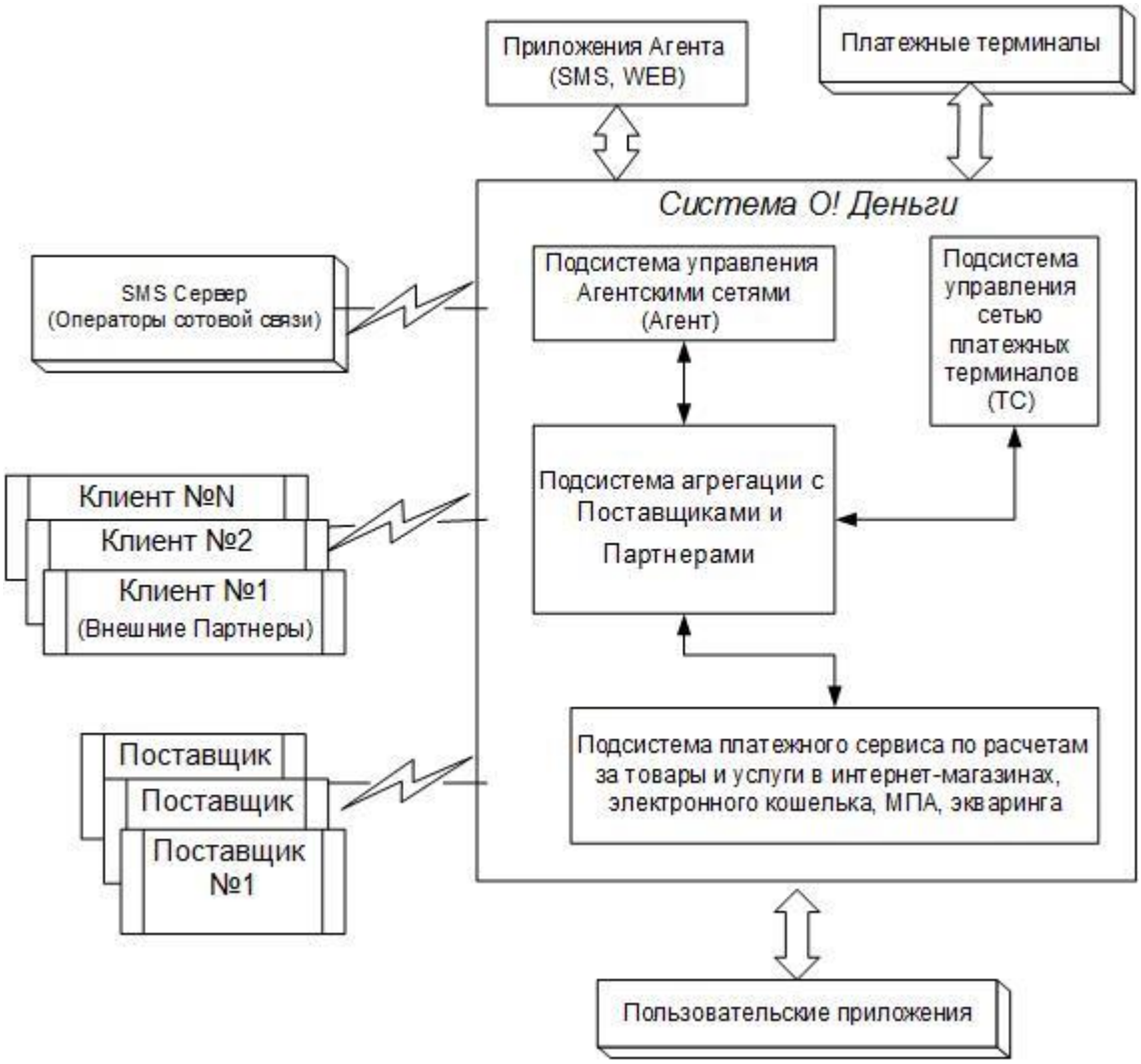
При выявлении фактов внешних угроз, преступлений, мошенничества в Платежной системе, которое может угрожать другим Участникам, незамедлительно производится уведомление Управления платежных систем НБКР по телефонным каналам связи, по электронной почте и любому другому средству связи доставки сообщений адресату.

Оператор обеспечивает своевременное доведение информации по принятым в систему платежам до поставщика товаров/услуг при возникновении нештатной ситуации в соответствии с условиями договора и требованиями нормативных правовых актов Национального банка.

Приложение №3
к Правилам Платежной Системы

Архитектура Системы «О!Деньги».

Архитектура системы «О!Деньги» имеет модульную структуру, ориентированную на обеспечение задач бесперебойного функционирования платежной системы, где каждая из подсистем закрывает свой назначенный функционал задач. Взаимодействие подсистем осуществляется посредством автоматизированного протокола взаимодействия заданного формата и условий реагирования на различные состояния процессов обработки платежных транзакций и состояния систем.



Назначение ИС:

- Мониторинг и управление АПК
- Обеспечение доступности и мониторинг сервисов и услуг платежного процессинга
- Обеспечение доступности и мониторинг взаимодействия участников платежного процессинга
- Интеграция, мониторинг и взаимодействие модулей системы
- Администрирование АПК
- Обеспечение бесперебойности и доступности 24/7/365

- Обеспечение своевременной передачи платежей и сообщений между участниками платежного процессинга
- Обеспечение целостности и безопасности платежного процессинга.

*Подсистема управления сетью платежных терминалов (**ТС**)* – специализированная информационная система для обеспечения проведения платежных операций плательщиками через сеть платежных терминалов в пользу поставщиков услуг и сервисов, осуществления мониторинга управления сетью платежных терминалов.

Назначение подсистемы:

- приём платежей от населения за услуги/товары с использованием платёжных терминалов в автоматическом режиме
- мониторинг и управление состоянием сети платежных терминалов
- техническое обслуживание и инкассирование платежных терминалов
- администрирование системы по конфигурации сети терминалов
- администрирование системы по предоставляемым услугам и комиссиям
- наличие оперативной отчетности по состоянию платежных транзакций, терминалов, настроек сети

Подсистема управления агентскими сетями («Система Агент») – специализированная информационная система для: обеспечения проведения платежных операций плательщиками посредством мобильного телефона, web приложения компьютера в пользу поставщиков услуг и сервисов
осуществления управления агентскими группами, балансами групп, контроля доступа и пр.

Назначение подсистемы:

- приём платежей от населения за услуги/товары посредством sms и web ресурсов
- администрирование системы по видам платежей
- мониторинг и управление состоянием агентской сети
- наличие оперативной отчетности по состоянию платежных транзакций, балансов Агентов и пр.
- интеграция с системой агрегации

Подсистема Агрегации с Поставщиками и Партнерами - специализированная информационная система для обеспечения передачи информации о платежных транзакциях в адрес поставщиков услуг и сервисов. Механизмы и формат передачи сведений о каждой платежной транзакции, операционное обслуживание платежной транзакции определяется с учетом требований регламента технологического взаимодействия Поставщиков товаров и услуг.

Назначение подсистемы:

- интеграция и мониторинг взаимодействия с Поставщиками
- обеспечение передачи сведений от Клиентов о каждой платежной транзакции в адрес Поставщиков услуг
- управление сетью клиентов и поставщиков
- управление системным и клиентскими каталогами сервисов и услуг
- обеспечение доступности сервисов и услуг
- интеграция и мониторинг взаимодействия с Клиентами
- администрирование системы по предоставлению доступа пользователям, Клиентам, Поставщикам

- наличие оперативной отчетности по Поставщикам, Клиентам, транзакциям

Подсистема платежного сервиса по расчетам за товары и услуги в интернет-магазинах, электронного кошелька, МПА, эквайринга - специализированная информационная система для обеспечения проведения платежей с помощью персонального компьютера, коммуникатора или мобильного телефона, виртуальной картой (опционально), представляет собой универсальный платежный кошелек позволяющий осуществлять расчеты за товары и услуги в интернет-магазинах, а также осуществления платежей по всем направлениям платежных и банковских услуг, по которым имеется соответствующая интеграция.

Для пользователей МПА:

- оплата коммунальных услуг (услуги по теплоснабжению, электроснабжению, газоснабжению, водоснабжению, канализации, обслуживанию лифтов, обслуживанию домофонов, вывозу бытовых отходов и др. услуги, где пользователь идентифицирован в силу договора между поставщиком услуг и пользователем услуги).
- пополнение банковских счетов (карт, выпущенных банками Кыргызской Республики).
- оплата налогов, сборов, госпошлин, штрафов и иных платежей в бюджет.
- оплата за интернет и телевидение.
- погашение кредитов и займов, полученных в банках и финансово-кредитных организациях Кыргызской Республики.
- услуги фиксированной связи.
- услуга подключения водителей Taxi (пополнение личного счета).
- оплата за сдачу электронной отчетности государственным органам Кыргызской Республики.
- оплата за получение государственных и муниципальных услуг.
- оплата покупки билетов (кино, транспорт и пр.) и услуг такси, кроме билетов на международный наземный и воздушный транспорт.
- оплата за бытовые услуги/товары/работы/сервисы, оказываемые/поставляемые/ выполняемые резидентами Кыргызской Республики внутри Кыргызской Республики, имеющими расчетный счет в коммерческих банках Кыргызской Республики.

Обеспечение безопасности информационного взаимодействия

Взаимодействие с Поставщиками: в дополнение к парольной защите и жесткой привязке провайдеров к IP-адресу АПК Оператора использует защищенное HTTPS соединение в режиме клиента.

Взаимодействие с Агентами: в дополнение к парольной защите используется защищенное HTTPS соединение в режиме клиента.

Взаимодействие с терминалами: в дополнение к парольной защите используется защищенное HTTPS соединение в режиме клиента. Политику генерации и распределения секретных ключей проводит специально назначенное лицо, и никто из третьих лиц не имеет доступа к ним.

Взаимодействие с другими Участниками: в дополнение к парольной защите используется защищенное HTTPS соединение.

Оценка возникновение риска мошенничества при взаимодействии с Участниками и Агентами рассматривается по следующим направлениям:

- программное обеспечение систем Участников (последовательность и связность формирования транзакций, достоверность и целостность транзакций, проверка корректности транзакций, методы хранения ключей, и т. д);
- получение секретных ключей и паролей Участников;
- получение паролей Агентов;
- проверка уровня доступности платежной системы при техническом взаимодействии с Участниками.

Внутренний контроль несанкционированного доступа и мошенничества ориентирован на анализ всей цепочки движения денежных средств на предмет:

- возможных злоупотреблений и мошенничества;
- нарушения базовых принципов безопасности платежей – авторизации сторон взаимодействия;
- достоверности представленной информации по транзакции, обеспечения ее целостности на всех этапах ее обработки;
- логирования и подотчетности всех операций;
- формирования системы контролей, исключающих неавторизованный доступ к этим данным или их утечку;
- контроля избыточных прав доступа, недостатков в разграничении прав доступа, исключения отсутствия контроля действий персонала;
- контроля ввода, проверки целостности и достоверности информации, корректности ее обработки.

Приложение № 4
к Правилам Платежной Системы

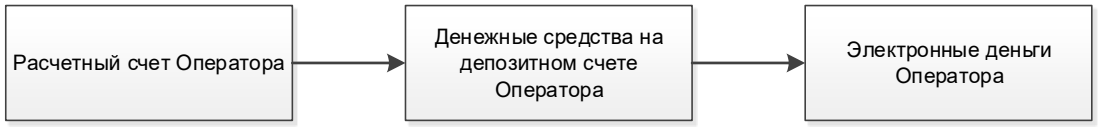
Порядок проведения процессинга.

1. Плательщик совершает платеж через терминальную систему. Плательщик при совершении платежа вводит в Клиентской части терминальной системы «О!Деньги» реквизиты. Под реквизитами понимается наименование Поставщика, в пользу которого совершается Платеж, Лицевой счет, а также сумма, подлежащая к оплате с целью обеспечения исполнения обязательств Абонента перед Поставщиком услуг /Получателем платежа;
2. Плательщик совершает платеж через Агента Оператора. Платежный Агент с помощью подсистемы «Агент» передает распоряжение Пользователя Оператору платежной системы (Платежной организации);
3. Плательщик совершает платеж через мобильное приложение и веб-сайт. Приложение позволяет комбинировать операции и выполнять действия «в один клик», формируя распоряжение Пользователя Оператору платежной системы (Платежной организации);
4. Если Платежный Лимит того Агента, через которого производится платеж (Терминальное оборудование, подсистема «Агент»), больше или равен сумме производимого платежа, в этом случае Информацию о Платеже (реквизиты платежа) передается в Процессинговый Центр (аппаратно-программный комплекс) Оператора. Передача Информации о платеже производится согласно внутреннего Протокола Оператора по обмену данными между Терминальным оборудованием/точкой приема платежей и Процессинговым центром. В случае Платежных терминалов, происходит периодическая проверка баланса Агента каждым из платежных терминалов Агента, на предмет превышения баланса Агента критического лимита. В случае если баланс Агента не превышает критического лимита, происходит блокирование приема платежей Платежным Терминалом вплоть до момента, когда размер Платежного лимита Агента вновь станет большим или равным критического лимита;
5. Процессинговый Центр Оператора передает Информацию о Платеже в аппаратно-программный комплекс Поставщика. Аппаратно-программный комплекс Поставщика на основании полученных данных (реквизитах платежа) от Оператора производит обработку Платежа. В случае, если переданная Информация (реквизиты платежа) корректна, Поставщик исполняет погашение обязательств Плательщика перед Поставщиком на сумму, полученную от Оператора по данному Платежу. В противном случае, исполнения обязательств Плательщика перед Поставщиком не происходит. Передача Информации о платеже от Оператора поставщику происходит согласно регламенту взаимодействия аппаратно-программного комплекса Оператора и Поставщика;
6. Аппаратно-программный Комплекс Поставщика уведомляет Процессинговый центр Оператора об успешности или не успешности проведения Платежа. Уведомление происходит по согласованному Сторонами регламенту взаимодействия аппаратно-программного комплекса Оператора и Поставщика;
7. Терминальное оборудование получит от Процессингового центра Оператора ответ о результате проведения Платежа согласно внутреннего Протокола Оператора по обмену данными между Терминальным оборудованием/ и Процессинговым центром;
8. В случае успешности обработки Платежа Поставщиком, Поставщик, при наличии в его аппаратно-программном комплексе такой функциональной возможности, направляет уведомление Плательщику об исполнении обязательств Плательщика перед Поставщиком на сумму Платежа;
9. Процессинговый центр «О!Деньги» обладает функционалом, который имеет технологическую возможность осуществлять проверку введенного Плательщиком лицевого счета Плательщика (сведения, позволяющего однозначно идентифицировать Плательщика) при совершении им (Плательщиком) Платежа, на присутствие лицевого счета в «Черном списке» лицевых счетов. В «Черный список» вносятся те счета (в том числе в качестве таких лицевых счетом могут

использоваться ФИО Плательщика), которые фигурируют в списках террористов, выпускаемых международными организациями, национальным списком террористов, национальным списком подозреваемых в причастности к терроризму, выдаваемых соответствующими органами. В случае обнаружения введенного Плательщиком лицевого счета при обработке Оператором Платежа в вышеуказанных списках, Оператор заблокирует дальнейшую Обработку Платежа, без передачи Поставщику Сведений о совершенном Плательщиком Платеже.

Порядок обеспечения процессинга с использованием электронных денег

1. Эмиссия электронных денег
   - Для приобретения электронных денег Оператор направляет банку-эмитенту запрос на приобретение необходимой суммы электронных денег.
   - Перед приобретением электронных денег Оператор размещает в банке-эмитенте гарантийный взнос, равный объему планируемой эмиссии.
   - Банк-эмитент проводит эмиссию электронных денег и пополняет котловой счет электронных денег Оператора платежной системы (Платежной организации). При этом объем котлового счета электронных денег не может превышать объем гарантийного взноса.
   - Банк-эмитент имеет полный доступ к Платежной системе Оператора для контроля соответствия объема электронных денег размеру гарантийного взноса.



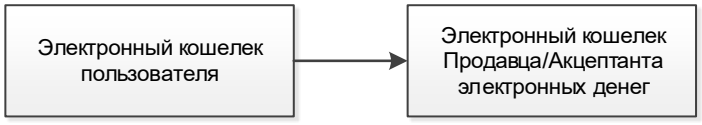
2. Пополнение электронного кошелька

   - Пользователь пополняет счет своего электронного кошелька путем передачи Оператору платежной системы (Платежной организации) денежных средств для зачисления на свой электронный кошелек.
   - Денежные средства для зачисления на свой электронный кошелек могут быть переданы следующими способами:
     - Перечислением с банковского счета; с банковской карты пользователя.
     - Переводом с идентифицированного электронного кошелька, предоплаченной карты и/или виртуальной предоплаченной карты;
     - Денежным переводом без открытия банковского счета через системы денежных переводов, прошедших регистрацию в Национальном банке Кыргызской Республики;
     - Внесением наличных денежных средств в автоматизированные терминалы самообслуживания (cash-in), в кассы Банка-эмитента, а также агентам коммерческих банков и/или Платежным Агентам.
   - Оператор платежной системы (Платежная организация) пополняет электронный кошелек Пользователя, используя свой котловой счет. При этом, сумма на котловом счете уменьшается на сумму, равную сумме пополнения электронного кошелька пользователя.
   - Агент может взымать комиссию за пополнение электронного кошелька пользователя.

3. Оплата услуг и покупка товаров с использованием электронных денег.

- Пользователь может покупать товары и оплачивать услуги Акцептантов электронных денег.
- Покупка товаров и оплата услуг происходит путем перевода электронных денежных средств с кошелька Пользователя на кошелек Акцептанта.

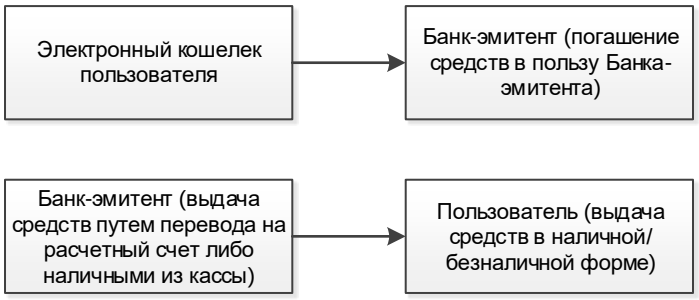
Схематично процесс представлен ниже:



4. Погашение электронных денежных средств с электронного кошелька

- Для погашения электронных денежных средств Пользователь должен обратиться в отделение Банка-эмитента с заявлением на погашение электронных денежных средств установленного образца со своего электронного кошелька.
- Погашение средств доступно только для идентифицированных электронных кошельков.
- Погашение электронных денежных средств проходит по следующей схеме – при обращении в банк-эмитент Пользователь предъявляет документы, удостоверяющие личность, а также сообщает сумму погашения. Банк-эмитент осуществляет погашение электронных денег в свою пользу. После погашения средств Банк-эмитент выдает Пользователю денежные средства наличными в кассе либо в безналичной форме путем перевода средств на банковский счет Пользователя.

Схематично процесс показан ниже:



Приложение №5
к Правилам Платежной Системы

Тарифная политика.

Тарифная политика отражает общие цели Оператора, которые он стремится достичь, формируя цены предоставляемых услуг.

При формировании цен на товары учитываются общеэкономические критерии, определяющие отклонения цен в ту или иную сторону от потребительной стоимости платежных услуг.

Эти критерии можно подразделить на внутренние (зависящие от руководства и различных служб предприятия) и внешние (не зависящие от самого предприятия и находящиеся за его пределами).

К критериям внутреннего характера можно отнести:

- качество сервиса;
- имидж Оператора.

Внешние критерии выглядят следующим образом:

- социальная значимость сервиса
- наличие и расширение рынка платежных услуг
- Участники и их требования к рынку платежных услуг
- нормативное регулирование
- политическая стабильность государства;
- наличие и уровень конкуренции
- другие факторы

Используется метод определения цен с ориентацией на спрос, уровень конкуренции и требования Участников. Оператор использует комбинированной системы методов определения цены одновременно с решением задачи развития сети платежных услуг, сети точек и способов приема платежей. Структура тарифов, комиссий и вознаграждений должна удовлетворять цели достижения уровня рентабельности, установленной Оператором.

В определённых случаях, продиктованных требованиями поставщиков услуг и товаров (в том числе, государственных и бюджетных предприятий), спросом и уровнем цен на тарифы, комиссии и вознаграждения, в отношении услуг, оказываемых платежными организациями и операторами платежных систем Кыргызской Республики, а также решениями Общества - структура тарифов, комиссий и вознаграждений может отличаться от установленного уровня рентабельности.

Перед определением тарифов, комиссий и вознаграждения проводится рыночный анализ спроса и уровня цен на тарифы, комиссии и вознаграждения, оказываемые платежными организациями и операторами платежных систем Кыргызской Республики

Уведомление Участников и пользователей о применяемых тарифах, комиссиях и вознаграждениях осуществляется согласно настоящим Правилам, договору Участника.

Оператор платежной системы один раз в год с момента получения лицензии предоставляет в Национальный банк сведения об утвержденных и действующих тарифах. Оператор платежной системы должен в течение 10 (десяти) рабочих дней после изменения тарифов уведомлять Национальный банк обо всех изменениях действующих тарифов.