Утверждены приказом
Директора за № F-23/04
от 14.06.2023 г.

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ «FusionPay»

Алматы 2023 год

ОГЛАВЛЕНИЕ

Общие положения (Термины и определения)

Настоящие правила осуществления деятельности товарищества с ограниченной ответственностью «FusionPay» в качестве платежной организации (далее – «правила» и «платежная организация» соответственно) разработаны в соответствии с Законом Республики Казахстан «О платежах и платежных системах» (далее – Закон о платежах), Постановлением Правления Национального банка Республики Казахстан № 215 от 31 августа 2016 года «Об утверждении Правил организации деятельности платежных организаций», Постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 202 «Об утверждении Правил выпуска, использования и погашения электронных денег, а также требований к эмитентам электронных денег и системам электронных денег на территории Республики Казахстан», другими нормативными правовыми актами Республики Казахстан, и определяют порядок организации деятельности платежной организации, включающий оказание платежных услуг платежной организацией, взаимодействие платежной организации с третьими лицами, в том числе с физическими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией, а также процедуры урегулирования спорных ситуаций и разрешения споров с клиентами при оказании платежных услуг.

Термины и понятия, используемые в настоящих правилах, употребляются в значениях, указанных ниже:

- **Клиент/Плательщик** – физическое лицо, обладающее надлежащей дееспособностью в соответствии с законодательством Республики Казахстан для осуществления платежа, совершившее конклюдентные действия, направленные на заключение договора об оказании услуг, и обладающее аутентификационными данными для доступа к системе в целях управления своей учетной записью, и последующего оказания платежной организацией платежных услуг, предусмотренных настоящими правилами.
- **Агент системы электронных денег/Агент** - банк, организация, осуществляющая отдельные виды банковских операций, Национальный оператор почты, платежная организация и платежный агент, осуществляющие деятельность по приобретению электронных денег у эмитента и владельцев - физических лиц для последующей их реализации физическим лицам на основании договора, заключенного с эмитентом электронных денег либо оператором системы электронных денег.
- **Платежная услуга** – услуга, оказываемая платежной организацией клиенту в соответствии с Законом Республики Казахстан «О платежах и платежных системах».
- **Риск** – присущая деятельности платежной организации возможность (вероятность) возникновения убытков, ухудшения ликвидности или иных негативных последствий вследствие наступления неблагоприятных событий, связанных с внутренними факторами (сложность организационной структуры, уровень квалификации работников, организационные изменения, текучесть кадров и т.д.) и внешними факторами (изменение экономической конъюнктуры, применяемые новые технологии, внедрение новых продуктов и т.д.).
- **Оценка риска** – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и/или совокупных рисков (группы рисков), принимаемых на себя платежной организацией.
- **Оферта** – договор на предоставление услуг Эмитентом/Оператором/Агентом физическим лицам по выпуску, использованию и погашению электронных денег, являющийся договором присоединения согласно положениям статьи 389 Гражданского кодекса Республики Казахстан, размещенный на интернет-ресурсах Оператора. В рамках настоящих Правил к Договорам присоединения относятся и договоры, которые по усмотрению Оператора могут заключаться в порядке, предусмотренном законодательством, Оператором с Участниками расчетов - физическими лицами и Агентами на предоставление Оператором услуг Платежной организации электронных денег, с их размещением на интернет-ресурсе Эмитента/Оператора/Агента.

- ✔ **Авторизация** – разрешение Оператора на проведение Владельцем электронных денег операций с использованием электронных денег в платежной организации, включая предоставление доступа в его личный кабинет. Процедура прохождения авторизации устанавливается Оператором.
- ✔ **Расчетный банк/Банк** – банк второго уровня, с которым платежная организация заключила договоры в целях оказания платежных услуг.
- ✔ **Банк-эмитент/Эмитент** – Эмитент, осуществляющий выпуск и погашение электронных денег в системе «FusionPay».
- ✔ **Банк-эквайер** – банк, обеспечивающий проведение операций по платежным картам.
- ✔ **Бенефициарный собственник** – физическое лицо:
  - которому прямо или косвенно принадлежат более 25 процентов долей участия в уставном капитале либо размещенных (за вычетом привилегированных и выкупленных обществом) акций клиента - юридического лица или иностранной структуры без образования юридического лица;
  - осуществляющее контроль над клиентом иным образом;
  - в интересах которого клиентом совершаются операции с деньгами и (или) иным имуществом;
- ✔ **Выпуск/эмиссия электронных денег** – выдача Банком электронных денег Участникам расчетов - физическим лицам/Клиентам и Агентам путем обмена на равную по их номинальной стоимости сумму денег.
- ✔ **Владелец электронных денег или Владелец ЭД**:
  - физическое лицо, резидент или нерезидент, достигшее шестнадцатилетнего возраста, получившее электронные деньги от Эмитента, Агента или от иных физических лиц – Участников расчетов;
  - Агенты;
  - Поставщики услуг, получившие электронные деньги от Участников расчетов - физических лиц в качестве оплаты по гражданско-правовым сделкам. Права Владельца электронных денег возникают с момента получения электронных денег.
- ✔ **Международные платежные системы (МПС)** – международные платежные системы: Visa International и MasterCard International и иные МПС.
- ✔ **Система по учету платежей (Система)** – совокупность программно-технических средств платежной организации, обеспечивающих информационно-технологическое взаимодействие, регистрацию и осуществление платежей и иных операций в соответствии с настоящими правилами.
- ✔ **Транзакция** – финансовая операция с картой, либо электронными деньгами в результате которой производится оплата каких-либо товаров или услуг, или перевод.
- ✔ **Шлюз** – программное обеспечение для создания электронного канала, посредством которого производится обмен данными по транзакциям и данными.
- ✔ **Товар** – товары, работы, услуги, права на результаты интеллектуальной деятельности, реализуемые поставщиком услуг конечным потребителям (клиентам) для личного, семейного или домашнего использования.
- ✔ **Платежная организация** – Товарищество с ограниченной ответственностью «FusionPay» (БИН 220640044701), созданное и действующее в соответствии с законодательством Республики Казахстан.
- ✔ **Система электронных денег «FusionPay» (Система ЭД)** – это совокупность программно-технических средств, документации и организационно-технических мероприятий, обеспечивающих осуществление платежей и иных операций с использованием электронных денег.
- ✔ **Оператор системы электронных денег «FusionPay»/Оператор** – ТОО «FusionPay», осуществляющее управление платежной организацией и обеспечивающее ее функционирование, включая осуществление сбора, обработки и передачи информации, формируемой при осуществлении операций с использованием электронных денег. Операции

с электронными деньгами – эмиссия, распространение, использование и погашение электронных денег.

- ✔ **Бесперебойность функционирования платежной организации** – комплексное свойство платежной организации «FusionPay», обозначающее ее способность предупреждать нарушения надлежащего функционирования (в том числе не допускать приостановления (прекращения) осуществления операций или ненадлежащего осуществления операций), а также восстанавливать надлежащее функционирование в случае его нарушения.
- ✔ **Поставщик услуг/Партнер** – юридическое лицо или физическое лицо, зарегистрированное в качестве индивидуального предпринимателя, заключившее отдельный договор с платежной организацией, и в пользу которого Клиент осуществляет платеж в счет оплаты за Товары, либо физическое лицо, принимающее денежные средства от Клиента, не связанные с предпринимательской деятельностью.
- ✔ **Процедуры безопасности** – комплекс организационных мер и программно-технических средств защиты информации, предназначенных для удостоверения прав Владельца электронных денег на использование электронных денег и обнаружения ошибок и/или изменений в содержании передаваемых и получаемых электронных сообщений при использовании электронных денег.
- ✔ **Инцидент информационной безопасности** – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов платежной организации.
- ✔ **Использование электронных денег** – передача электронных денег в платежную организацию их Владельцем - физическим лицом другому Участнику расчетов в целях осуществления платежа по гражданско-правовым сделкам и (или) иных операций, связанных с переходом права собственности на электронные деньги.
- ✔ **Личный кабинет** – персональный раздел Владельца электронных денег на интернет-ресурсе платежной организации «FusionPay», посредством которого владелец электронных денег, Поставщик услуг, имеет доступ к своему электронному кошельку для получения необходимой информации об остатке электронных денег, операциях, проведенных по нему, осуществления платежей и иных операций с использованием электронных денег в порядке, предусмотренном настоящими Правилами и заключенными договорами. Перечень предоставляемых услуг посредством личного кабинета Владельца электронных денег устанавливается Оператором.
- ✔ **Третьи лица** – юридические лица и физические лица – индивидуальные предприниматели, которые предоставляют технологическое обеспечение платежных услуг или иным образом действуют в интересах платежной организации, и не являются аффилированными с платежной организацией.
- ✔ **Участники расчетов или Участники** – Эмитент, Агент, Оператор, Клиент, физические лица (резиденты и нерезиденты, достигшие шестнадцатилетнего возраста) и Поставщики услуг, принявшие обязательство по соблюдению Правил платежной организации «FusionPay».
- ✔ **Погашение электронных денег** – платежная услуга, предусматривающая осуществление Эмитентом электронных денег обмена выпущенных им электронных денег, предъявленных владельцем электронных денег, либо подлежащих обмену без их предъявления владельцем в случаях, предусмотренных законами Республики Казахстан, на равную по их номинальной стоимости сумму денег.
- ✔ **Электронные деньги/ЭД** - безусловные и безотзывные денежные обязательства Эмитента, хранящиеся в электронной форме и принимаемые в качестве средства платежа в платежной организации «FusionPay» другими Участниками. Электронные деньги номинированы в национальной валюте Республики Казахстан – тенге.
- ✔ **Электронный кошелек** – учетная запись Клиента/Агента/Поставщика услуг в системе электронных денег, обеспечивающая посредством совокупности программно-технических средств (включая, но не ограничиваясь: web-интерфейс, мобильные приложения и приложения для планшетных компьютеров, программное обеспечение Терминалов и пр.) хранение

Электронных денег Клиента/Агента/Поставщика услуг и/или доступ Клиента/Агента/Поставщика услуг к Электронным деньгам.

✔ **Электронное сообщение** – любое сообщение, составленное электронным способом и передаваемое между Участниками расчетов, по защищенному каналу связи.

1. Описание платежных услуг, оказываемых платежной организацией.

1.1. Услуги по реализации (распространению) электронных денег, оказываются Платежной организацией на основании договоров об оказании платежных услуг, заключаемых Платежной организацией с эмитентом электронных денег, в соответствии с условиями которых Платежная организация выступает агентом системы электронных денег, и осуществляет деятельность по приобретению электронных денег у эмитента и владельцев - физических лиц для последующей их реализации Клиентам - физическим лицам в соответствии с Законом о платежах.

Услуги по реализации (распространению) электронных денег оказываются посредством внесения Клиентом наличных денежных средств через электронные терминалы (устройства) платежных агентов/субагентов, и/или с использованием иных средств электронного платежа, перечень которых размещен на сайте Системы.

1.2. Услуги по приему и обработке платежей, совершаемых с использованием электронных денег, оказываются Платежной организацией на основании договоров заключаемых платежной организацией с эмитентом электронных денег, и платежной организацией с третьими лицами, обеспечивающими информационно-технологическое обеспечение для оказания платежной услуги. Платежная организация, является Оператором системы электронных денег, оферта системы электронных денег размещена на сайте www.fusionpay.kz.

1.3. Услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам осуществляются Платежной организацией на основании отдельных договоров, заключенных с банком/ банками второго уровня и платежной организацией с третьими лицами и обеспечивает прием платежей инициированных с использованием платежных карт с указанием реквизитов назначения соответствующего платежа и бенефициара соответствующего платежа с последующим обеспечением передачи реквизитов по платежу для его исполнения в адрес соответствующего банка, а банк в свою очередь исполняет указание Клиента, переданное через Систему Платежной организации в электронной форме.

2. Порядок и сроки оказания платежных услуг Клиентам платежной организации.

2.1. Порядок оказания услуги по реализации (распространению) электронных денег.

Для приобретения электронных денег, Клиенту необходимо произвести регистрацию электронного кошелька. Регистрация происходит по Абонентскому номеру.

Для регистрации электронного кошелька Клиенту необходимо ознакомиться с условиями публичного договора-оферты эмитента электронных денег (далее – «Оферта»), ссылка на который размещена на Сайте Системы, и, в случае согласия с условиями, Клиент осуществляет полный и безоговорочный акцепт Оферты.

Совершая действия, на регистрацию электронного кошелька Клиент принимает условия Оферты, а также в полном объеме и без каких-либо изъятий принимает условия публичной оферты об оказании услуг безналичных платежей с использованием электронных денег эмитента электронных денег в рамках системы электронных денег «FusionPay».

Регистрация электронного кошелька клиента в Системе ЭД, а также приобретение электронных денег, и последующее пополнение баланса электронного кошелька, происходит путем пополнения Клиентом электронного кошелька наличными через электронные терминалы

платежных агентов/субагентов, банкоматы, через финансовые интернет-порталы, а также с использованием платежных карт и иных способов электронного платежа, перечень которых размещен на Сайте Системы.

Выпуск Электронных денег осуществляется исключительно Эмитентом в пределах суммы денег, полученной от Клиентов или Агентов с учетом ограничений, установленных действующим законодательством Республики Казахстан.

В момент реализации электронных денег Клиенту выдается квитанция или иной документ, подтверждающий факт приобретения Клиентом электронных денег.

Электронные деньги считаются реализованными Клиенту с момента отражения информации о доступном остатке электронных денег в электронном кошельке Клиента.

Сроки оказания платежной услуги – от 1 (одного) до 3 (трех) рабочих дней с момента получения денег от физических лиц, электронные деньги реализуются физическому лицу с отражением в электронном кошельке владельца электронных денег.

2.2. Порядок оказания услуги по приему и обработке платежей, совершаемых с использованием электронных денег.

В системе ЭД Платежная организация является оператором системы ЭД. Согласно Оферте Оператора системы ЭД, размещенной на сайте www.FusionPay.kz Оператор системы ЭД оказывает Клиентам услуги по приему, обработке платежей, совершаемых с использованием электронных денег.

В целях оказания платежной услуги, Клиенту необходимо пройти регистрацию в Системе ЭД и осуществить приобретение электронных денег. После регистрации учетной записи Клиента в Системе ЭД и приобретения электронных денег, Клиент вправе осуществлять использование Системы ЭД, в том числе осуществлять доступ к Балансу учетной записи в целях совершения платежей.

Совершение платежей производится Клиентом путем формирования, удостоверения и передачи посредством Системы ЭД распоряжения с использованием Электронных денег о совершении платежа в пользу конкретного Получателя платежа в электронном виде.

После проверки корректности, введенных Клиентом Аутентификационных данных, Кодов подтверждения или команд, переданных посредством Message-подтверждения, а также достаточности суммы электронных денег на балансе Учетной записи Клиента для совершения платежа, Платежная организация передает информацию, указанную Клиентом в распоряжении Эмитенту, а также уведомляет Клиента о принятии к исполнению, либо об отказе от исполнения соответствующего распоряжения эмитентом электронных денег.

Исполнение Эмитентом распоряжений Клиента о совершении платежа осуществляется на условиях, установленных Публичной Офертой об оказании услуг безналичных платежей с использованием Электронных денег эмитентом электронных денег в рамках системы ЭД «FusionPay».

Платежная организация обязуется фиксировать в электронном регистре учета возникновение, изменение или прекращение взаимных прав и обязательств сторон по Договору оказания услуг, заключаемому Клиентом путем присоединения к Оферте через совершение конклюдентных действий, предусмотренных Офертой.

Информирование Клиента о совершении каждого платежа производится путем размещения информации в соответствующем разделе Учетной записи Клиента, доступ к которой предоставлен Клиенту на Сайте Системы. Клиент обязуется проверять информацию в соответствующем разделе не менее 1 (одного) раза в день. В случае если Клиент не проверяет информацию о совершении платежей в соответствующем разделе на Сайте Системы, Платежная организация не несет ответственности в связи с тем, что Клиент не получил информацию об операции. Клиент признает и акцептом Оферты подтверждает, что с момента размещения информации о совершении платежа в соответствующем разделе на Сайте Системы обязательство Платежной организации по информированию Клиента исполнено надлежащим образом.

Платежная организация также может направлять Клиенту SMS-оповещения об операциях по списанию (за исключением операций по списанию оплаты в пользу Платежной организации) и операциях по пополнению Учетной записи Клиента на Абонентский номер, указанный при регистрации Учетной записи Клиента.

2.2.1. Регистрация в Системе электронных денег «FusionPay» Партнеров, принимающих к оплате электронные деньги.

Для принятия к оплате Партнером электронных денег заключается договор о партнерстве на прием электронных денег эмитентом электронных денег (далее - «Эмитент») по форме, согласованной между Партнером и Эмитентом.

Для регистрации Партнера в Системе ЭД, Партнер осуществляет следующие действия:

1. Партнер заполняет анкету поставщика услуг для подключения к Системе ЭД;
2. После подачи анкеты происходит процедура согласования и подписания договора между Партнером, Платежной организацией и Эмитентом.
3. На основании присвоенного id Партнера производится подключение к Системе ЭД.

2.2.2. На ежеквартальной основе формируется и передается отчет для эмитента и Национального Банка Республики Казахстан, формируемый в соответствии с установленными нормативными правовыми актами Национального банка Республики Казахстан и договором, заключенным между Оператором и эмитентом.

2.2.3. Порядок отражения электронных кошельков в Системе ЭД (схема денежных и информационных потоков).

Выпуск Электронных денег осуществляется исключительно Эмитентом в пределах суммы денег, полученной от Клиентов или Агентов с учетом ограничений, установленных действующим законодательством Республики Казахстан.

При внесении денег Клиент указывает номер Электронного кошелька, открытый в Системе ЭД, на который зачисляются приобретаемые им электронные деньги.

В случае внесения денег третьими лицами для зачисления электронных денег на Электронный счет Клиента, права и обязанности в отношении приобретенных/безвозмездно полученных электронных денег возникают у Клиента - владельца электронного кошелька. Данные действия оцениваются как совершенные третьими лицами в интересах владельца электронного кошелька.

Оператор обеспечивает соответствие общей суммы денег, принятых от Клиентов отраженной на его балансовом счете, сумме электронных денег, находящейся на позиции Эмитента в Системе ЭД.

Электронные деньги Клиента считаются выпущенными Эмитентом с момента отражения информации о доступной сумме электронных денег в Электронном кошельке.

Платежная организация осуществляет проверку полученных от Эмитента данных и отражает указанную в электронном сообщении Эмитента сумму выпуска электронных денег на позиции Эмитента в Системе ЭД и на Электронном кошельке Клиента.

2.2.4. Использование и погашение электронных денег.

Электронные деньги используются их владельцем в целях осуществления платежей по гражданско-правовым сделкам, а также проведения иных операций на условиях, определенных Правилами и не противоречащих законодательству Республики Казахстан.

Платежи и иные операции с использованием электронных денег осуществляются их владельцем в пользу идентифицированного владельца электронных денег.

Электронные деньги, владельцем которых является неидентифицированное физическое лицо, не подлежат реализации агенту (приобретению агентом).

У Партнеров, получившего электронные деньги в системе электронных денег при совершении гражданско-правовых сделок, возникает право денежного требования к эмитенту электронных денег в сумме принятого платежа.

Максимальная сумма одной операции, совершаемой неидентифицированным владельцем электронных денег - физическим лицом, не должна превышать сумму, равную пятидесятикратному размеру месячного расчетного показателя, установленного на соответствующий финансовый год в согласно законодательству Республики Казахстан.

Максимальная сумма одной операции, совершаемой упрощенно идентифицированным владельцем электронных денег - физическим лицом, не должна превышать сумму, равную стократному размеру месячного расчетного показателя, установленного на соответствующий финансовый год, согласно законодательству Республики Казахстан.

Максимальная сумма одной операции, совершаемой владельцем электронных денег - индивидуальным предпринимателем или юридическим лицом, не должна превышать сумму, равную тысячекратному размеру месячного расчетного показателя, установленного на соответствующий финансовый год, согласно законодательству Республики Казахстан.

Максимальная сумма электронных денег, хранимых на одном электронном устройстве неидентифицированного владельца электронных денег - физического лица, не превышает сумму, равную стократному размеру месячного расчетного показателя, установленного на соответствующий финансовый согласно законодательству Республики Казахстан.

Сумма электронных денег, хранимых на электронном кошельке упрощенно идентифицированного владельца электронных денег - физического лица, не должна превышать сумму, равную трехсоткратному размеру месячного расчетного показателя, установленного на соответствующий финансовый год, согласно законодательству Республики Казахстан.

Общая сумма платежей и (или) иных операций с использованием электронных денег с электронного кошелька неидентифицированного владельца электронных денег - физического лица в течение рабочего дня не должна превышать сумму, равную стократному размеру месячного расчетного показателя, установленного на соответствующий финансовый год согласно законодательству Республики Казахстан.

Общая сумма платежей и (или) иных операций с использованием электронных денег с электронного кошелька упрощенно идентифицированного владельца электронных денег - физического лица на электронный кошелек идентифицированного либо упрощенно идентифицированного владельца электронных денег в течение рабочего дня не должна превышать сумму, равную трехсоткратному размеру месячного расчетного показателя, установленного на соответствующий финансовый год согласно законодательству Республики Казахстан.

2.2.4.1. Погашение электронных денег

Эмитент принимает на себя безусловное и безотзывное денежное обязательство по погашению выпущенных им электронных денег в соответствии с их номинальной стоимостью в национальной валюте Республики Казахстан.

Погашение электронных денег осуществляется Эмитентом путем перечисления равной по их номинальной стоимости суммы денег на банковский счет Клиента - владельца электронных денег - физического лица либо выдачи ему наличных денег.

Для погашения электронных денег на банковский счет Клиента - владельца электронных денег посредством мобильного приложения и/или Сайта Системы Клиент формирует указание о погашении электронных денег, в котором указывает сумму электронных денег к погашению и указывает банковский счет, на который следует осуществить погашение электронных денег.

Платежная организация направляет указание Клиента эмитенту для осуществления процедуры погашения. Эмитент, перед погашением осуществляет процедуру проверки указанного владельцем электронных денег банковского счета, на который следует погасить электронные деньги.

Операции по погашению электронных денег неидентифицированным владельцам электронных денег недоступны. В случае инициирования клиентом операции по погашению электронных денег клиенту будет направлено уведомление о невозможности проведения такой операции, с предложением пройти процедуру полной идентификации либо упрощенной

идентификации с указанием адресов, по которым может обратиться владелец электронных денег для прохождения полной идентификации.

2.2.4.2. Порядок закрытия электронного кошелька в системе электронных денег.

При закрытии электронного кошелька Клиентом в мобильном приложении и/или на Сайте Системы формируется указание о закрытии Электронного кошелька с указанием способа вывода электронных денег (при наличии такой возможности) в наличной и/или безналичной форме. В случае, если Клиент неидентифицирован, для закрытия Электронного кошелька ему необходимо пройти процедуру идентификации/упрощенной идентификации. После прохождения такой процедуры Клиент отправляет указание о закрытии Электронного кошелька и о выводе электронных денег способами, указанными выше. После погашения электронных денег Платёжная организация направляет указание Клиента о закрытии Электронного кошелька Эмитенту для закрытия электронного кошелька.

В случае отсутствия электронных денег на Электронном кошельке Клиента, прохождение процедуры идентификации для закрытия Электронного кошелька не требуется.

2.2.4.3. Полная и упрощенная идентификация владельца электронных денег - физического лица.

Процедура Идентификации в Системе электронных денег «FusionPay» делится на упрощенную идентификацию и полную.

Полная идентификация владельца электронных денег производится эмитентом/Оператором электронных денег при личном присутствии владельца электронных денег и предъявлении им документа, удостоверяющего личность, либо посредством удаленной идентификации на основании сведений из доступных источников, полученных от операционного центра межбанковской системы переводов денег, а также иным способом, не противоречащим требованиям законодательства Республики Казахстан.

Идентификация включает осуществление следующих мер:

1) фиксирование сведений, необходимых для идентификации физического лица, совершающего операцию с деньгами или иным имуществом и (или) иным имуществом: данные документа, удостоверяющего его личность, индивидуальный идентификационный номер, а также юридический адрес;

2) фиксирование сведений, необходимых для идентификации юридического лица, совершающего операцию с деньгами или иным имуществом и (или) иным имуществом: данные справки о государственной (учетной) регистрации (перерегистрации) юридического лица, учредительных документов, бизнес-идентификационный номер, характер деятельности, а также адрес места нахождения;

3) фиксирование сведений, необходимых для идентификации иностранной структуры без образования юридического лица, совершающего операцию с деньгами или иным имуществом и (или) иным имуществом: наименование, номер (при наличии), под которым иностранная структура без образования юридического лица зарегистрирована в иностранном государстве (на территории), адрес места нахождения, место ведения основной деятельности, характер деятельности, а в отношении трастов и иных иностранных структур без образования юридического лица с аналогичной структурой или функцией также состав имущества, находящегося в управлении (собственности), фамилия, имя, отчество (если оно указано в документе, удостоверяющем личность) и адрес места жительства (места нахождения) учредителей (участников) иностранной структуры без образования юридического лица и бенефициарных собственников (при наличии);

4) выявление бенефициарного собственника и фиксирование сведений, необходимых для его идентификации, в соответствии с подпунктом 1) настоящего пункта, за исключением юридического адреса.

Упрощенная идентификация:

Идентификация Клиента упрощенным способом осуществляется путем проведения сеанса видеоконференции или путем фиксирования изображения Клиента с помощью

специализированного приложения, реализующего технологию выявления движения, интервьюируемого в процессе идентификации.

Упрощенная идентификация осуществляется посредством официального интернет-ресурса и (или) мобильного приложения Эмитента и/или Оператора.

Во время проведения упрощенной идентификации Эмитент и/или Оператор обеспечивает:

полное фиксирование лица владельца электронных денег - физического лица и документа, удостоверяющего его личность;

получение из открытых источников подтверждения об индивидуальном идентификационном номере владельца электронных денег - физического лица.

Сроки оказания платежной услуги – от 1 (одного) до 3 (трех) рабочих дней с момента получения денег от физических лиц, электронные деньги реализуются физическому лицу с отражением в электронном кошельке владельца электронных денег.

2.3. Порядок оказания услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам.

Услуга по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам осуществляется следующим образом:

1. Прием информации о платежах инициированных с использованием платежных карт с указанием реквизитов назначения соответствующего платежа и бенефициара соответствующего платежа с последующим обеспечением передачи реквизитов по платежу для его исполнения в пользу соответствующего банка-эквайера, а банк-эквайер в свою очередь исполняет указание клиента, переданное через Систему Платежной организации в электронной форме. При этом платежная организация оказывает услуги по сбору, обработке и рассылке информации участникам расчетов по операциям с платежными карточками.
2. Инициация Клиентом операций/ платежей производится посредствам WEB – приложений, online - приложений, мобильных приложений (приложений для мобильных устройств), программного обеспечения, терминалов самообслуживания, виджетов и прочих приложений - обеспечивающих возможность инициации клиентом в электронной форме распоряжений на списание денег с платежной карты клиента, с целью последующего исполнения поручения/ распоряжения Клиента полученного Платежной организацией от Клиента и переданного Платежной организацией в Банк.
3. При оказании платежной услуги Платежная организация обеспечивает следующий алгоритм действий:

- Клиент посредством сети интернет/ мобильного телефона заходит в соответствующее приложение/сайт Поставщика услуг;
- Клиент знакомится с условиями предоставления платежной услуги и соглашается с условиями Оферты на платежной странице;
- Клиент в приложении/сайте инициирует платеж в пользу Поставщика услуг;
- Клиент вводит персональные данные в приложении/сайте Поставщика услуг;
- Для оплаты платежа Клиент вводит реквизиты банковской карты;
- Платежная организация посредством запроса в Банк инициирует распоряжение Клиента, полученного в электронной форме;
- Банк-эквайер, получив подтверждение от Платежной организации производит списание с банковской карты Клиента, и перевода Платежа в пользу Поставщика услуг, указанного в поручении Клиента, сумму инициируемой Клиентом операции с учетом вознаграждения Платежной организации или перевод платежа со счета банка – эквайера на специальный счет Расчетного банка, с которым у Платежной организации заключен соответствующий договор.

- После зачисления платежей на специальный счет Платежная организация передает в электронном виде Расчетному банку поручение с указанием суммы и реквизитов Поставщика услуг, которому необходимо зачислить платежи, после чего Расчетный банк осуществляет перевод платежей на расчётный счет Поставщика услуг.
- Платежная организация получает от Банка подтверждение исполнения Операции;
- Платежная организация выдает Клиенту электронный чек, подтверждающий совершение Клиентом операции.

Перевод банком на текущий счет Поставщика услуг по совершенным транзакциям производится банком в национальной валюте Республики Казахстан.

Сроки оказания платежной услуги - в течение 1 (одного) рабочего дня, следующего за днем приема платежа.

2.4. Платежная организация осуществляет следующие действия при оказании платежной услуги по переводу денег:

2.4.1. Со специального счета Расчетного банка, с которым у платежной организации заключен соответствующий договор, на карту Клиента:

- Платежная организация в ежедневном круглосуточном режиме реального времени принимает запросы на переводы (Выплаты) от Поставщиков услуг.
- По факту получения такого запроса, Платежная организация передает банку, с которым у платежной организации заключен соответствующий договор, информацию о списании денег со специального счета и зачислении денег на платежную карточку Клиента (получателя).
- Банк, по получению информации от платежной организации осуществляет перевод денег со специального счета на платежную карточку Клиента (получателя).
- Платежная организация и Банк осуществляют обработку операций, в сроки и в соответствии с Правилами МПС.
- Платежная организация в режиме реального времени информирует Клиентов о результате оказания услуги в отношении каждой конкретной операции.

2.4.2. С корпоративной карты Поставщика услуг на карту Клиента:

- Платежная организация в ежедневном круглосуточном режиме реального времени принимает запросы на переводы (Выплаты) от Клиентов.
- По факту получения такого запроса, Платежная организация передает банку, с которым у платежной организации заключен соответствующий договор, информацию о списании денег с корпоративной карточки Поставщика услуг (отправителя) и зачислении денег на платежную карточку Клиента (получателя).
- Банк, по получению информации от платежной организации, осуществляет перевод денег с одной платежной карточки на другую, оператором по переводам является Банк.
- Платежная организация и Банк осуществляют обработку операций, в сроки и в соответствии с Правилами МПС.
- Платежная организация в режиме реального времени информирует Клиентов о результате оказания услуги в отношении каждой конкретной операции.

Перевод считается принятым и становится окончательным с момента направления Держателю платежной карточки (Клиенту) подтверждения об осуществлении перевода (квитанция о переводе).

3. Стоимость платежных услуг (тарифы), оказываемых платежной организацией

Тарифы платежной организации ТОО «FusionPay» по платежным услугам:

3.1. Услуги по реализации (распространению) электронных денег:

№	Категория сервиса	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента.
1.	Реализация (распространение) электронных денег	от 0 % до 15% от суммы реализованных электронных денег

3.2. Услуги по приему и обработке платежей, совершаемых с использованием электронных денег:

№	Категория сервиса	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента.
1.	Прием и обработка платежей, совершаемых с использованием электронных денег	от 0 до 1% для физических лиц; Для юридических лиц – указывается в Тарифной политике Платежной организации и в Договоре

3.3. Услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам:

№	Наименование категорий сервисов, предоставляемых Поставщиками услуг при осуществлении деятельности по интернет эквайрингу	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента.
1.	Интернет - магазины	От 0 до 6% от суммы операции
2.	Букмекеры	От 0 до 6% от суммы операции
3.	Сотовые операторы	От 0 до 6% от суммы операции
4.	Интернет и телефония	От 0 до 6% от суммы операции
5.	Билеты (авиа, ж/д)	От 0 до 6% от суммы операции
6.	МКО	От 0 до 10% от суммы операции
7.	Места общественного питания, рестораны, магазины, супермаркеты, салоны красоты и прочие виды сервисов, не включенные в отдельные категории	От 0% до 15% от суммы операции

3.3.1. Услуги по переводу денег (Выплаты):

№	Наименование категорий сервисов, предоставляемых Поставщиками услуг при осуществлении деятельности по оказанию платежной услуги по переводу денег	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента.
1.	Интернет - магазины	От 0 до 3% от суммы операции, минимум/фикс. 300 тг от суммы операции

2.	Букмекеры	От 0 до 3% от суммы операции, минимум/фикс. 300 тг от суммы операции
3.	Сотовые операторы	От 0 до 3% от суммы операции, минимум/фикс. 300 тг от суммы операции
4.	Интернет и телефония	От 0 до 3% от суммы операции, минимум/фикс. 300 тг от суммы операции
5.	МКО	От 0 до 3% от суммы операции, минимум/фикс. 300 тг от суммы операции
6.	Места общественного питания, рестораны, магазины, супермаркеты, салоны красоты и прочие виды сервисов, не включенные в отдельные категории	От 0% до 5% от суммы операции, минимум/фикс. 300 тг от суммы операции

Детали формирования, порядок установления комиссий/дополнительных комиссий, взимаемых с Клиента/Поставщика услуг, а также полный список сервисов, устанавливается в соответствии с Тарифной политикой, утвержденной Платежной организацией, договорными условиями, указанными в договорах, заключенных между ТОО «FusionPay» и поставщиками услуг, и иными лицами, предоставляющими услуги Клиентам.

4. Порядок взаимодействия с банками, Поставщиками услуг, платежными агентами и третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией.

4.1. Порядок взаимодействия Платежной организации при работе с Поставщиками услуг.

- проводятся маркетинговые исследования, включающие в себя анализ рынка, конкурентоспособности, потребительскую способность;
- финансовой службой проводится экономическое обоснование заведения нового Поставщика услуг в систему Платежной организации, а также выявляется платежная нагрузка на Клиентов;
- после проведения вышеуказанных действий и принятия положительного решения по работе с Поставщиком услуг, у последнего запрашиваются все необходимые документы в рамках соблюдения требований закона РК «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и проводится полный анализ комплаенс рисков.
- в случае отсутствия комплаенс рисков производится обмен технической документацией для подключения Поставщика услуг к системе Платежной организации по протоколу технического взаимодействия API.

4.1.1. Заключение договора с Поставщиком услуг.

– После проведения всех действий в соответствии с п. 4.1. настоящих Правил между Платежной организацией и Поставщиком услуг заключается Договор, либо Поставщик услуг присоединяется к публичному Договору, опубликованному на сайте www.FusionPay.kz.

– Платежной организацией заключается договор с Поставщиком услуг об оказании платежных услуг и/или Договор технического взаимодействия с обязательным наделением правом Платежной организации о принятии платежа на специальный счет Расчетного банка, с которым у платежной организации заключен соответствующий договор в пользу Поставщика услуг, а также обязательно предусматривается возможность привлечения Платежной организацией Платежных агентов/субагентов.

– Поставщик услуг проходит регистрацию в Системе, с присвоением ID.

– Платежная организация обязана передавать Поставщику услуг данные о каждом принятом платеже для внесения изменений в лицевой счет клиента. Сведения должны быть

переданы непосредственно в период приема платежа на основании данных, указываемых клиентом, без ошибок и искажений.

– Каждая операция по передаче данных о платеже сопровождается подписанием Платежным агентом/субагентом электронного документа, форма которого согласована с соответствующим Поставщиком услуг. Сочетание аутентификационных данных – логин, пароль и/или номер терминала в Системе - определены как аналог собственноручной подписи (далее АСП) Платежной организации и признаются сторонами в качестве однозначного и бесспорного подтверждения совершенного платежа.

– При приеме платежей Платежной организации взимается комиссия с платежа. Размер комиссии устанавливается Платежной организацией, и определяется условиями работы с Поставщиками услуг.

4.2. Порядок взаимодействия Платежной организации с Банками.

Платежная организация заключает с Банком договор о взаиморасчетах и информационно техническом взаимодействии.

Платежная организация проходит регистрацию в Системе Банка, для чего:

– В согласованный сторонами договора срок Платежная организация осуществляет реализацию Интерфейса подключения (API) к Системе Банка;

– Стороны проводят техническое тестирование систем;

– Сторонами определяется техническая готовность систем к отправке информации о платежах;

– Платежная организация обязана передавать данные Банку о каждом обработанном платеже;

– Банк обязан передавать Платежной организации данные о каждом обработанном платеже;

– Сведения должны быть переданы непосредственно в период обработки платежа;

– Каждой операции по передаче данных о платеже присваивается уникальный номер в Системе Банка;

– Платежная организация с Банком проводит ежедневную сверку по обработанным платежам;

– На ежемесячной основе производится сверка взаиморасчетов.

Детализированное описание передвижения денежных средств при положительно обработанной операции оплаты:

– Банк-эмитент осуществляет списание денег с Карты Плательщика;

– Банк – эмитент осуществляет перевод платежа в пользу Банка-эквайера.

Банк-эквайер перечисляет платеж на расчетный счет Поставщика услуг или на специальный счет Расчетного банка, с которым у платежной организации заключен соответствующий договор, Расчетный банк осуществляет перевод со специального счета на расчетный счет Поставщика услуг.

4.3. Порядок взаимодействия при работе с Платежным агентом (при возникновении производственной необходимости).

– Финансовой службой проводится экономическое обоснование заведения нового Платежного агента в систему Платежной организации, а также выявляется платежная нагрузка на Клиентов.

– После проведения вышеуказанных действий и принятия положительного решения по работе с Платежным агентом, у последнего запрашиваются все необходимые документы в рамках ПОД/ФТ и проводится полный анализ комплаенс рисков.

– В случае отсутствия комплаенс рисков производится обмен технической документацией для подключения Платежного агента к системе Платежной организации по протоколу технического взаимодействия API.

4.3.1. Заключение договора с Платежным агентом.

После проведения всех действий в соответствии с п. 4.3. настоящих Правил между Платежной организацией и Платежным агентом заключается Договор.

– Платежной организацией заключается договор с Платежным агентом об оказании платежных услуг с обязательным наделением правом Платежного агента о принятия платежа в пользу Поставщика услуг, а также обязательно предусматривается возможность привлечения Платежным агентом Платежных субагентов.

– Платежный агент проходит регистрацию в Системе, с присвоением ID.

– Оказание платежной услуги обеспечивается предоставлением Платежным агентом гарантийного взноса (авансового платежа) на планируемый объем принятия платежей. При совершении платежа клиентом, сумма принятых платежей списывается с расчетного счета (баланса) в системе Платежной организации.

– Платежный агент обязуется обеспечивать на указанном счете неснижаемый остаток денежных средств, достаточный для исполнения обязательств перед Платежной организацией.

– При отсутствии в день приема платежей денежных средств в остатке гарантийного взноса Платежного агента, обязательство Платежного агента является необеспеченным, и Платежная организация вправе приостановить исполнение договора либо предоставить Платежному агенту отсрочку в перечислении платежа (коммерческий кредит, либо овердрафт) на основании отдельного соглашения, заключаемого платежной организацией с поставщиком услуг или гарантийного письма.

– Платежный агент обязан передавать Платежной организации данные о каждом принятом платеже для внесения изменений в лицевой счет клиента. Сведения должны быть переданы непосредственно в период приема платежа на основании данных, указываемых клиентом, без ошибок и искажений.

– При приеме платежей Платежным агентом взимается комиссия с платежа. Размер комиссии устанавливается Платежной организацией, и определяется условиями работы с поставщиками услуг.

4.4. Третьи лица — это юридические лица и индивидуальные предприниматели, которые:

- предоставляют услуги платежной организации или действуют в интересах платежной организации;
- не входят в группу компании платежной организации и не являются работниками платежной организации.

Подключение информационных систем третьей стороны к системам платежной организации производится на основании заключенного договора на оказание информационных и\или технологических услуг и соглашения о неразглашении конфиденциальной информации.

Соглашение о неразглашении конфиденциальной информации устанавливает обязанность третьей стороны соблюдать конфиденциальность информации, а также ответственность за разглашение конфиденциальной информации, к которой она получает доступ.

Заключаемый договор или соглашение о неразглашении конфиденциальной информации должны учитывать типовые положения по исполнению третьей стороной требований по обеспечению информационной безопасности. Требования должны включать как минимум следующее:

- ответственность и обязательства за поддержание требуемого уровня информационной безопасности;
- мероприятия по уведомлению об инцидентах информационной безопасности и нарушениях в системе защиты информации.

5. Сведения о системе управления рисками, используемой Платежной организацией

Система управления рисками направлена на обеспечение финансовой устойчивости и стабильного функционирования Платежной организации, и представляет собой систему организации, политик, процедур и методов, принятых Платежной организацией, и позволяющих Платежной организации своевременно осуществлять выявление, измерение, контроль, мониторинг за возникающими рисками, и разработка мероприятий по минимизации рисков при оказании платежных услуг.

В целях эффективного управления рисками, работа платежной организации состоит из систематической работы по разработке и практической реализации мер по предотвращению и минимизации рисков, выявлению, измерению, контролю и мониторингу рисков, оценки эффективности их применения, а также контролю за совершением всех денежных операций. В указанных целях в Платежной организации закреплен работник (в случае отсутствия такого работника, данные функции выполняет первый руководитель), выполняющий функции по управлению рисками, в задачи которого входит:

✔ **Анализ и оценка рисков, включающих в себя систематическое определение: объектов анализа рисков; индикаторов риска по объектам анализа риска, определяющих необходимость принятия мер по предотвращению и минимизации рисков;** оценки возможного ущерба в случае возникновения рисков;

✔ Разработка и реализация практических мер по управлению рисками с учетом: вероятности возникновения рисков и возможных последствий; анализа применения возможных мер по предотвращению и минимизации рисков.

При разработке процедур выявления, измерения мониторинга и контроля за рисками платежная организация учитывает, но не ограничивается следующими факторами:

1) размер, характер и сложность бизнеса;
2) доступность рыночных данных для использования в качестве исходной информации;
3) состояние информационных систем и их возможности;
4) квалификацию и опыт персонала, вовлеченного в процесс управления рыночным риском.

Процедуры выявления, измерения, мониторинга и контроля за рисками охватывают все виды активов, обязательств; охватывают все виды рыночного риска и их источники; позволяют проводить на регулярной основе оценку и мониторинг изменений факторов, влияющих на уровень рыночного риска, включая ставки, цены и другие рыночные условия; позволяют своевременно идентифицировать рыночный риск и принимать меры в ответ на неблагоприятные изменения рыночных условий.

Основная задача регулирования рисков в платежной организации - это поддержание приемлемых соотношений прибыльности с показателями безопасности и ликвидности в процессе управления активами и пассивами платежной организации, т.е. минимизация потерь.

Эффективное управление уровнем риска в платежной организации должно решать целый ряд проблем - от отслеживания (мониторинга) риска до его стоимостной оценки. Уровень риска, связанного с тем или иным событием, постоянно меняется из-за динамичного характера внешнего окружения платежной организации. Это заставляет платежную организацию регулярно уточнять свое место на рынке, давать оценку риска тех или иных событий, пересматривать отношения с клиентами и оценивать качество собственных активов и пассивов, следовательно, корректировать свою политику в области управления рисками. Процесс управления рисками в платежной организации включает в себя: предвидение рисков, определение их вероятных размеров и последствий, разработку и реализацию мероприятий по предотвращению или минимизации, связанных с ними потерь. Все это предполагает разработку платежной организацией собственной стратегии управления рисками таким образом, чтобы своевременно и последовательно использовать все возможности развития платежной организации и одновременно удерживать риски на приемлемом и управляемом уровне.

Цели и задачи стратегии управления рисками в большой степени определяются постоянно изменяющейся внешней экономической средой, в которой приходится работать.

В основу управления рисками положены следующие принципы:

- ✔ прогнозирование возможных источников убытков или ситуаций, способных принести убытки, их количественное измерение;
- ✔ финансирование рисков, экономическое стимулирование их уменьшения;
- ✔ ответственность и обязанность руководителей и сотрудников, четкость политики и механизмов управления рисками;
- ✔ координируемый контроль рисков по всем подразделениям платежной организации, наблюдение за эффективностью процедур управления рисками.

Система управления рисками характеризуется такими элементами как мероприятия и способы управления.

Мероприятия по управлению рисками:

1) определение организационной структуры управления рисками, обеспечивающей контроль за выполнением партнерами платежной организации требований к управлению рисками, установленных правилами управления рисками платежной организации;

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

3) доведение до органов управления платежной организации соответствующей информации о рисках;

4) определение показателей бесперебойности функционирования платежной организации;

5) определение порядка обеспечения бесперебойности функционирования платежной организации;

6) определение методик анализа рисков;

7) определение порядка обмена информацией, необходимой для управления рисками;

8) определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;

9) определение порядка изменения операционных и технологических средств и процедур;

10) определение порядка оценки качества функционирования операционных и технологических средств, информационных систем;

11) определение порядка обеспечения защиты информации в платежной организации.

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

Способы управления рисками:

1) управление очередностью исполнения распоряжений должностными лицами;

2) осуществление расчета в платежной организации до конца рабочего дня;

3) обеспечение возможности предоставления лимита;

4) использование безотзывных банковских гарантий;

5) отказ от взаимодействия с неблагонадежными партнерами;

6) страхование возможных рисков;

7) соблюдение Платежной Организацией и его работниками требований законодательства Республики Казахстан о ПОД/ФТ и правил внутреннего контроля;

8) другие способы управления рисками.

6. Порядок урегулирования спорных ситуаций и разрешения споров с Клиентами

В случае возникновения у Клиента каких-либо претензий к Платежной организации по любой спорной ситуации, связанной с оказанием платежных услуг, клиент вправе направить платежной организации соответствующую претензию в письменной форме.

Клиент обязан обратиться к платежной организации с письменным заявлением, составленным в произвольной форме, содержащим указание на возникшую спорную ситуацию (далее – «Претензия») путем направления его почтовым отправлением по адресу - 050042, Республика Казахстан, город Алматы, Ауэзовский район, улица Пятницкого, дом 83, кв. 45.

При каждом направлении платежной организации Претензии клиента, она подлежит регистрации платежной организацией путем присвоения даты и порядкового номера входящей корреспонденции. Датой приема Претензии клиента платежной организации считается фактическая дата регистрации входящего обращения клиента.

Обращения в службу технической поддержки клиентом по телефону, направления сообщений через форму обратной связи в приложении системы не могут быть признаны обращением к платежной организации с Претензией и (или) расцениваться как досудебное урегулирование споров.

Ко всем Претензиям, направляемым клиентами платежной организации, должны быть приложены надлежащим образом оформленные копии документов, подтверждающие факты, указанные в заявлении, а также следующие документы:

1. нотариально заверенная копия документа, удостоверяющего личность клиента;
2. документ, подтверждающий оплату (чек).
3. дополнительно может быть запрошена нотариально заверенная копия договора об оказании услуг сотовой связи, заключенного с оператором сотовой связи и предоставляющего клиенту право использования абонентского номера, указанного клиентом при регистрации учетной записи клиента в системе и др.

Платежная организация рассматривает полученную Претензию клиента и подготавливает ответ для направления в срок не более 30 (тридцати) календарных дней со дня получения соответствующей Претензии клиента.

1. Для надлежащего рассмотрения Претензии клиента и подготовки ответа платежная организация:
2. привлекает к всестороннему изучению спора сотрудников компетентных подразделений (технических, правовых, расчетных, и иных структурных подразделений для получения разъяснений, дополнительных сведений и иных данных в отношении оспариваемой ситуации);
3. запрашивает и получает от клиента дополнительно документы (или их копии), объяснения и иные сведения. По запросу платежной организации клиент обязан предоставить запрашиваемые платежной организацией сведения и документы (их копии) в целях надлежащего досудебного урегулирования возникшего спора;
4. проводит тщательный анализ полученных сведений и разъяснений для формирования полного и достоверного ответа на Претензию клиента;
5. подготавливает мотивированный письменный ответ клиенту на Претензию.

Любой спор, если он не был разрешен мирным путем в досудебном порядке, подлежит окончательному разрешению в судебном порядке в соответствии с действующим законодательством Республики Казахстан.

7. Порядок соблюдения мер информационной безопасности

7.1. Меры информационной безопасности – это средства и меры предотвращения несанкционированного доступа к программно – техническим средствам, применяемые в платежной организации, в том числе программно-технические средства защиты, обеспечивающие необходимый уровень защиты информации и сохранения ее конфиденциальности в соответствии с требованиями, установленными законодательством Республики Казахстан и предполагающие скоординированную деятельность сотрудников платежной организации.

Методами обеспечения защиты информации в платежной организации являются:

Препятствие – метод физического преграждения и доступа к оборудованию, носителям информации с использованием организационных и технических мер, включая организацию службы охраны и режима, применения системы контроля и управления доступом, системы видеонаблюдения, охранной и пожарной сигнализации, системы пожаротушения и др.

Управление доступом – метод защиты информации регулированием использования всех ресурсов автоматизированной информационной системы предприятия. Управление доступом включает следующие функции защиты:

Идентификация пользователей, персонала и ресурсов информационной системы.

Аутентификация – установление подлинности объекта или субъекта по предъявленному им идентификатору.

Проверка полномочий – проверка соответствия дня недели, времени суток, запрашиваемых ресурсов и процедур установленному регламенту.

Регистрация (протоколирование) обращений к защищаемым объектам и информации.

Маскировка – метод защиты информации в автоматизированной информационной системе предприятия путем ее криптографического закрытия.

Регламентация – метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможность несанкционированного доступа к ней сводилась бы к минимуму.

Защита информационной системы платежной организации осуществляется с целью исключения возможностей:

- ✔ нарушений законных интересов участников вследствие неблагоприятного стечения обстоятельств (наступления событий), связанных с внутренними и внешними факторами функционирования системы;
- ✔ внесения несанкционированных изменений в технические и программные средства системы;
- ✔ внесения несанкционированных изменений в электронные документы;
- ✔ появления в компьютерах компьютерных вирусов и программ, направленных на разрушение, нарушение работоспособности или модификацию программного обеспечения системы, либо на перехват информации, в том числе паролей.

7.2. Права администратора программно-аппаратных средств информационной безопасности к системе предоставляются уполномоченному сотруднику оператора, ответственному за обеспечение информационной безопасности организации.

7.3. Для обеспечения безопасности и конфиденциальности расчетов используются специальные процедуры, включающие:

- ✔ Наличие пароля для ограничения доступа к личному кабинету пользователя, обеспечивающего защиту информации от несанкционированной модификации или уничтожения.
- ✔ обеспечение безопасных условий эксплуатации аппаратно-программных средств и исключение несанкционированного доступа к ним.
- ✔ проведение расследований событий, вызвавших операционные сбои, анализ их причин и последствий;
- ✔ принятие мер по устранению или минимизации рисков информационной безопасности.
- ✔ контроль соблюдения требований правил, договорных обязательств участниками в части обеспечения бесперебойности работы и обеспечения безопасности системы;
- ✔ проведение внутренних и внешних аудитов для выявления уязвимостей, принятие мер по устранению выявленных уязвимостей.

7.4. Уровень риска информационной безопасности определяется в зависимости от степени угрозы и вероятности возникновения риска:

I (низкий) – уровень риска, в результате которого возможные/выявленные нарушения не оказывают влияние на информационную безопасность Платежной организации;

II (средний) – уровень риска, в результате которого возможные/выявленные нарушения оказывают влияние на информационную безопасность Платежной организации в незначительной мере;

III (допустимый) – уровень риска, в результате которого возможные/выявленные нарушения оказывают влияние на информационную безопасность Платежной организации в допустимой мере;

IV (высокий) – уровень риска, в результате которого возможные/выявленные нарушения оказывают влияние на информационную безопасность Платежной организации в значительной мере;

V (критический) - уровень риска, в результате которого возможные/выявленные нарушения могут привести к полному прекращению функционирования системы.

7.5. Требования по организации хранения и использования паролей:

7.5.1. Физические лица самостоятельно генерируют для себя пароль доступа к личному кабинету.

7.5.2. Участники системы - юридические лица должны определить перечень работников, уполномоченных сопровождать операции с использованием системы.

7.5.3. При назначении (изменении, в том числе временном) пользователь системы обязан произвести смену своего пароля.

7.5.4. Длина паролей должна составлять не менее восьми символов, состоящих из не менее двух заглавных букв, двух прописных букв, двух чисел и двух специальных знаков.

7.5.5. Носители ключевой информации (пароля доступа к личному кабинету) должны храниться только у тех лиц, которым они принадлежат.

7.5.6. Хранение и использование носителей ключевой информации должен исключать возможность несанкционированного доступа к ним.

7.5.7. Во время работы с носителями ключевой информации доступ к ним посторонних лиц должен быть исключен.

7.5.8. По окончании каждого рабочего сеанса пользователь должен «выходить» из кабинета.

7.5.9. В случае подозрения на компрометацию пароля доступа к личному кабинету необходимо незамедлительно произвести его замену.

7.6. Запрещается:

- ✔ передавать носители ключевой информации лицам, к ним не допущенным;
- ✔ выводить секретные ключи на дисплей или принтер;
- ✔ оставлять носитель ключевой информации без присмотра на рабочем месте.

7.7. Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению, и учету в системе отслеживания Jira ответственным специалистом информационной безопасности, а также дальнейшему недопущению повторения инцидента информационной безопасности. Срок хранения информации об инцидентах информационной безопасности составляет 5 (пять) лет.

В целях постоянного совершенствования соблюдения мер информационной безопасности в соответствии с полученной информацией об инцидентах информационной безопасности, платежной организацией в ходе мониторинга деятельности по обеспечению информационной безопасности требуется регулярно пересматривать соблюдение мер информационной безопасности – не реже одного раза в год. По результатам пересмотра в настоящие правила в случае необходимости вносятся соответствующие изменения.

Внеплановый пересмотр мер информационной безопасности может быть выполнен в случае внесения существенных изменений в информационную инфраструктуру платежной организации, а также по итогам расследования критичных инцидентов информационной безопасности.

Планирование системы информационной безопасности основывается на анализе информационных рисков, что позволяет обеспечить адекватность мер по защите информации по отношению к ценности защищаемых данных и актуальности соответствующих угроз. Для проведения анализа рисков осуществляется оценка и категорирование защищаемых данных, выявляются актуальные угрозы информационной безопасности, а также проводится анализ защищенности компонентов информационной инфраструктуры. На основе результатов анализа информационных рисков выбираются соответствующие меры по их обработке и дальнейшему совершенствованию.

Мониторинг функционирования методов защиты информации проводится с целью выявления инцидентов информационной безопасности и проверки соответствия практики применения защитных мер принятым планам обработки информационных рисков.

Для контроля эффективности выполнения документированных процедур информационной безопасности анализируются соответствующие контрольные следы (записи), свидетельствующие о результатах их выполнения.

Для проверки соответствия системы обеспечения информационной безопасности предъявляемым к ней требованиям проводится регулярный внутренний аудит со стороны ответственного сотрудника.

Результаты, полученные на этапе мониторинга, используются для совершенствования системы обеспечения информационной безопасности. Выявленные недостатки, несоответствия системы предъявляемым требованиям, а также зарегистрированные инциденты информационной безопасности подлежат тщательному изучению с целью выработки эффективных корректирующих и превентивных действий. Корректирующие и превентивные действия устраняют существующие и потенциальные недостатки системы обеспечения информационной безопасности платежной организации, что в итоге приводит к достижению основной цели – поддержанию и улучшению качества защиты информации.

7.8. Платежной организацией определяется порядок принятия неотложных мер к устранению инцидента информационной безопасности, его причин и последствий. Неотложные меры применяются в соответствии с возникшим инцидентом информационной безопасности и инициируются ответственным сотрудником платежной организации, включающим необходимый перечень организационных действий, направленный на своевременное реагирование и недопущение повторного инцидента информационной безопасности.

Платежная организация обязана принять следующие неотложные меры в отношении выявленных инцидентов, связанных с нарушением требований по информационной безопасности:

- предвидеть необходимые действия для принятия мер против возникновения инцидента информационной безопасности, которые могут произойти, и определить перечень действий;
- принять действенные меры в короткий срок, но не позднее 3 (трех) часов, в связи с произошедшим инцидентом информационной безопасности;
- обеспечение непрерывности работы при возникновении инцидента информационной безопасности, а также предотвращение незаконных платежей и несанкционированных изменений остатков на счетах, восстановление информации и устранение иных негативных ситуаций, связанных с последствиями инцидента информационной безопасности;
- обеспечение соблюдения сотрудниками платежной организации установленных требований информационной безопасности при работе в программно-технических средствах.

7.9. Ответственным сотрудником платежной организации ведется журнал учета инцидентов информационной безопасности в системе отслеживания Jira с отражением всей информации об инциденте информационной безопасности путем регистрации факта возникновения инцидента информационной безопасности (дата, время, описание события и прочее), принятых мерах и предлагаемых корректирующих мерах, связанных с недопущением повторного инцидента информационной безопасности.

В зависимости от инцидента информационной безопасности ответственный сотрудник осуществляет разделение инцидента информационной безопасности в журнале учета на внутренние и внешние инциденты информационной безопасности.

В случае возникновения повторного инцидента информационной безопасности, ответственный сотрудник, после проведения регистрации факта в журнале учета инцидентов информационной безопасности в системе отслеживания Jira, проводит дополнительные мероприятия с привлечением первого руководителя с целью выявления соответствующих уязвимостей и дальнейшему недопущению инцидента информационной безопасности.

Анализ причин возникновения инцидента информационной безопасности, отражаемых в журнале учета инцидентов информационной безопасности, связанного с нарушением требований информационной безопасности, включает в себя следующие мероприятия:

- порядок проведения анализа причин инцидента информационной безопасности ответственным сотрудником (должностным лицом, ответственным за обеспечение информационной безопасности) совместно с соответствующими подразделениями после принятия мер по выявленным инцидентам;

- предупреждение причин инцидентов информационной безопасности и разработка мер по предотвращению возникновения таких ситуаций или снижению возможности причинения вреда в случае их возникновения (в том числе с привлечением ответственного сотрудника);
- изучение соответствующих отчетов программно-технических средств и получение объяснений от сотрудников, вызвавших инцидент информационной безопасности (внутренние инциденты);
- классификация нежелательных явлений по степени негативного воздействия и их оценка на основе критериев оценки.

Ответственный сотрудник публикует и хранит в отдельном файле журнал учета инцидентов информационной безопасности, связанный с нарушением установленных требований информационной безопасности, меры, принятые в отношении тех или иных инцидентов, результаты их оценки и другую дополнительную информацию в соответствии с требованиями законодательства Республики Казахстан.

7.10. Платежная организация представляет в Национальный Банк Республики Казахстан информацию о выявленных инцидентах информационной безопасности в соответствии с требованиями законодательства Республики Казахстан.

7.11. Информация об инцидентах информационной безопасности, указанных в настоящем разделе, предоставляется ответственным сотрудником платежной организации не позднее 48 (сорока восьми) часов с момента выявления инцидента информационной безопасности по регламентированной форме согласно нормативно-правовым актам Республики Казахстан (Карта инцидента информационной безопасности). При этом каждый инцидент формируется отдельной формой инцидента информационной безопасности.

7.12. Информация по обработанным инцидентам информационной безопасности представляется в электронном формате с использованием платформы Национального Банка Республики Казахстан для обмена событиями и инцидентами информационной безопасности. Данное требование закреплено в соответствующих нормативно-правовых актах и должным образом обязано выполняться платежной организацией.

8. Описание программно-технических средств и оборудования, необходимого для осуществления платежных услуг

8.1. Программное обеспечение, используемое Платежной организацией обеспечивает соответствие требованиям к программно-техническим средствам платежной организации и системе управления информационной безопасностью.

8.2. Для целей обеспечения надежного хранения информации применяется дублирование систем хранения данных, а также наличием холодного резерва комплектующих к ним.

8.3. Защиту от несанкционированного доступа обеспечивают меры по ограничению прав пользователей на рабочих станциях (Админ, пользователь).

8.4. Обеспечение целостности баз данных и полную сохранность информации в электронных архивах и базах данных при полном или частичном отключении электропитания в любое время на любом участке оборудования обеспечивается хранением информации с использованием системы управления базой данных (далее – СУБД) Microsoft SQL Server версии не ниже Standard Edition выпуска не старше 2016.

8.5. Доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении предоставляется пользователям в соответствии с «Матрицей владельцев и администраторов информационных систем» определяющей как минимум следующие уровни доступа:

- Владелец;
- Администратор;
- Разработчик;
- Пользователь.

8.6. Требования к учетным записям пользователей:

1) учётные записи, включая системные и сервисные, в системном и прикладном программном обеспечении, а также системы и средства защиты информации (включая доступ к управлению межсетевыми экранами и антивирусным программным обеспечением) защищены стойкими методами аутентификации;

2) каждому пользователю информационной системы назначается уникальный идентификатор (имя учётной записи);

3) недопустимость использования разделяемых между несколькими пользователями учётных записей, групповых и общих учётных записей, паролей и других средств аутентификации.

8.7. В используемых формах ввода данных используется контроль полноты вводимых данных либо справочники полей обязательных к заполнению, необходимых для проведения и регистрации операций, в случае выполнения функций или операций без полного заполнения всех полей программа может обеспечивать запись в журнал и\или выдачу соответствующего уведомления.

8.8. Программное обеспечение, используемое для проведения и регистрации операций обеспечивает поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по доступным параметрам, а также возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе.

8.9. Обработка информации и ее хранение осуществляется по дате и времени.

8.10. Информационные системы, задействованные в проведении и хранении операций обеспечивают процесс формирования форм отчетов, представляемых операторами систем электронных денег в Национальный Банк Республики Казахстан, а также отчетов о проведенных операциях.

8.11. Резервированное копирование и восстановление данных, хранящихся в учетных системах, обеспечивается средствами используемых СУБД. Контроль выполнения процедур резервного копирования осуществляется путем:

- оповещения ответственного сотрудника при удачном\неудачном резервном копировании;
- тестирования восстановления баз данных информационных систем не реже 1 (одного) раза в год.

8.12. Программное обеспечение реализует возможность вывода выходных документов на экран, принтер или в файл.

8.13. Программное обеспечение реализует возможность обмена электронными документами.

8.14. Регистрацию и идентификацию происходящих в информационной системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события, результат выполнения события фиксируется средствами используемых СУБД, в том числе:

- модуль для сбора событий;
- модуль для анализа и управления событиями и потоками сети из устройств, конечных точек, серверов, антивирусов, брандмауэров и различных систем предотвращения вторжений.

9. Порядок внесения изменений в настоящие Правила

9.1. Изменения и/или дополнения в настоящие Правила могут вноситься как путем утверждения новой редакции, так и путем подготовки текста изменений и/или дополнений к Правилам.

9.2. Дата вступления в силу изменений и/или дополнений в правила определяется Платежной организацией.

9.3. В случае несогласия участника с изменениями и/или дополнениями в Правила или тарифами, участник вправе отказаться от дальнейшего использования платежными услугами Платежной организации.

9.4. Последующее внесение изменений и/или дополнений в правила осуществляется в порядке, установленном настоящим разделом правил.

9.5. Дальнейшее использование платежных услуг Платежной организации со стороны участника после вступления в силу любых изменений и/или дополнений в Правила означает согласие участников с такими изменениями и/или дополнениями.