

Утверждены

Решением №2 от «01» марта 2024 г.

Директора ТОО «Open Trade»

Сыздыкова Л.Н.



**ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ
ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ
ТОО «Open Trade»**

2024г.

ОГЛАВЛЕНИЕ

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ	1
Глава 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	3
Глава 3. ОПИСАНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ.....	6
Глава 4. ПОРЯДОК И СРОКИ ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ КЛИЕНТАМ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ.....	8
Глава 5. СТОИМОСТЬ ПЛАТЕЖНЫХ УСЛУГ (ТАРИФЫ), ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ	18
Глава 6. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ТРЕТЬИМИ ЛИЦАМИ, ОБЕСПЕЧИВАЮЩИМИ ТЕХНОЛОГИЧЕСКОЕ СОПРОВОЖДЕНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ.	21
Глава 7. СВЕДЕНИЯ О СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ, ИСПОЛЬЗУЕМОЙ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ.	24
Глава 8. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ И РАЗРЕШЕНИЯ СПОРОВ С КЛИЕНТАМИ	27
Глава 9. ПОРЯДОК СОБЛЮДЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	28
Глава 10. ОПИСАНИЕ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ И ОБОРУДОВАНИЯ, НЕОБХОДИМЫХ ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖНЫХ УСЛУГ.....	38
Глава 11 ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ.....	43

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие Правила осуществления деятельности платежной организации ТОО «Open Trade» (далее – Правила) разработаны в соответствии с Законом Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах» (далее – Закон о платежах), Правилами организации деятельности платежных организаций, утвержденными постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215 (далее – Правила № 215), Уставом ТОО «Open Trade» и определяют порядок организации деятельности ТОО «Open Trade» (далее - Товарищество или Платежная организация) в качестве платежной организации.

ГЛАВА 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В Правилах используются понятия, предусмотренные законами Республики Казахстан от 26 июля 2016 года «О платежах и платежных системах», от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан», от 7 января 2003 года «Об электронном документе и электронной цифровой подписи», от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», от 21 мая 2013 года «О персональных данных и их защите», Правилами организации деятельности платежных организаций, утвержденными постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 215 (далее – Правила № 215), а также следующие понятия:

1) **Товар** – товары, работы и услуги, а также права на результаты интеллектуальной деятельности, реализуемые Получателями платежа конечным потребителям (Пользователям) для личного, семейного или домашнего использования.

2) **Система по учету платежей (Система)** – совокупность программно-технических средств, обеспечивающих информационно-технологическое взаимодействие и регистрацию платежей, а также, оказывающая услуги по сбору, обработке, хранению и передаче информации о платежах участникам расчетов.

3) **Банк/Банк-эквайер** – Банк второго уровня, с которым Платежная организация заключила договор в целях 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 и обеспечивающий проведение Операций по платежным карточкам.

4) **Банк-эмитент** – банки, осуществляющие выпуск платежных карточек, в том числе Банк.

5) **Участники расчетов** – Мерчант, Держатель платежной карточки, Банк-эквайер.

6) **Держатель платежной карточки (Покупатель)** – законный держатель Карты, использующий Карту для совершения Операций.

7) **Международные платежные системы (МПС)** – международные платежные системы: Visa International, MasterCard International и иные МПС.

8) **Обработка платежей** – обработка ТОО «Open Trade» и Банком с применением АПК Банка и Системы, в соответствии с Правилами МПС информации об Операциях, которая включает в себя сбор, обработку и рассылку участникам расчетов (Банк-эквайер, Мерчант, Держатель карты) информации по совершенным Операциям.

9) **Операция (Операции)** – общее определение, включающее в себя следующие виды платежей с использованием платёжных карт: Операцию оплаты, Операцию отмены оплаты, Операцию возврата, Операцию отмены возврата.

10) **Клиент** - физическое и/или юридическое лицо, филиал или представительство юридического лица, индивидуальный предприниматель, обладающие надлежащей дееспособностью/правоспособностью в соответствии с действующим законодательством РК для совершения Платежа, совершившие конклюдентные действия, направленные на заключение Договора об оказании услуг посредством акцепта условий настоящей Оферты, и обладающее Аутентификационными данными для доступа к Системе для ее использования в целях управления Учетной записью Пользователя, осуществлению доступа к Электронным деньгам на Балансе Учетной записи Пользователя в целях совершения Платежей.

11) **Мерчант/Получатель платежа** – юридическое лицо или индивидуальный предприниматель, реализующий Товары Клиентам через интернет-магазин и заключивший договор с Платежной организацией.

12) **Риск** – присущая деятельности Платежной организации возможность (вероятность) понесения убытков, ухудшения ликвидности или возникновения 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, применение новые технологий, внедрение новых продуктов и т.д.).

13) **Процессинг** - обработка ТОО «Open Trade» и Банком с применением АПК в соответствии с Правилами МПС информации об Операциях, которая включает в себя сбор, обработку и рассылку участникам расчетов (Банк-эквайер, Мерчант, Держатель карты) информации по совершенным Операциям.

14) **АПК** – специализированный аппаратно-программный комплекс ТОО «Open Trade» и (или) Банка.

15) **Итоговый реестр платежей** – отчет в электронном виде, формируемый ТОО «Open Trade» и содержащий перечень всех платежей с указанием сумм за каждый календарный день (или дни, в случае если Итоговый реестр формируется за несколько выходных/нерабочих праздничных дней). Формат Итогового реестра платежей определяется ТОО «Open Trade» самостоятельно.

16) **Электронный кошелек** - учетная запись Клиента/Агента в Системе, 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 и/или доступ Клиента к электронным деньгам в целях осуществления платежей с их использованием. Порядок регистрации Электронного кошелька Клиента определяется Офертой Системы ЭД. Клиент имеет право одновременно зарегистрировать не более одного Электронного кошелька на один Абонентский номер.

17) **Абонентский номер** - номер мобильного (сотового) телефона, принадлежащий Клиенту в соответствии с договором об оказании услуг сотовой связи, заключенному с оператором сотовой связи и предоставляющего Клиенту право использования указанного мобильного (сотового) номера.

18) **Система электронных денег «Open Trade» (Система ЭД)** - совокупность программно-технических средств, документации и организационно-технических мероприятий, обеспечивающих осуществление платежей с использованием электронных денег путем взаимодействия Платежной организации, с Эмитентом электронных денег и (или) Клиентом (владельцами электронных денег), а также обеспечивающих предоставлению Клиенту (владельцу электронных денег) услуг по: (i) осуществлению доступа к Учетной записи Клиента в целях совершения платежей; (ii) сбору, обработке, хранению и предоставлению Клиенту консолидированной информации о совершенных платежах; (iii) информированию (по поручению Клиента) Получателей платежа о совершенных Клиентом платежах; а также иных информационно-технологических услуг, непосредственно связанных с поименованными выше и необходимых для их корректного оказания. Система ЭД позволяет осуществлять регистрацию Учетной записи Клиента, а также управление ею. Организация работы Системы ЭД и оказание услуг по учету взаимных прав и обязательств ее участником производится Платежной организацией, являющейся оператором Системы ЭД.

19) **Аутентификационные данные** – уникальные имя Клиента (login), пароль (password), и/или код подтверждения, используемые для доступа к Системе, в том числе к Системе ЭД, через сеть Интернет, и/или через электронный терминал платежного агента/субагента, и/или через мобильное приложение, и совершения операций в пределах суммы денежных средств, доступной Пользователю в целях предъявления Эмитенту требований об осуществлении расчетов. Аутентификационные данные присваиваются Клиенту в момент регистрации Пользователя в Системе.

20) **Код подтверждения** – уникальная последовательность цифр и/или букв, предоставляемая Клиенту Платежной организацией посредством SMS-сообщения на Абонентский номер, указанный Клиентом при регистрации в Системе, в целях подтверждения платежа. Код подтверждения предоставляется Платежной организацией Клиенту для каждого платежа в порядке, предусмотренном Офертой Системы ЭД.

21) **Учетная запись** - запись в аналитическом учете Системы ЭД, связанная с Электронным кошельком Клиента, представляющая собой средство учета электронных денег, как поступающих на Электронный кошелек Клиента, так и расходуемых Клиентом при совершении платежей. Идентификатором Учетной записи Клиента в Системе ЭД выступает Абонентский номер.

22) **Партнер** - юридическое лицо и (или) индивидуальный предприниматель принимающие электронные деньги в качестве оплаты за поставляемые ими товары, работы и услуги.

23) **Информация об инцидентах информационной безопасности, включая сведения о нарушениях, сбоях в информационных системах** – информация об отдельно или серийно возникающих сбоях в работе информационно- коммуникационной инфраструктуры или отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов платежной организации;

24) **Инцидент информационной безопасности, включая нарушения, сбои в информационных системах (далее - 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 их получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов платежной организации;

25) **Информационная безопасность** – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз;

26) **Угроза информационной безопасности** – совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

27) **Обеспечение информационной безопасности** – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов платежной организации;

28) **Периметр защиты информационно-коммуникационной инфраструктуры** – совокупность программно-аппаратных средств, отделяющих информационно-коммуникационную инфраструктуру платежной организации от внешних информационных сетей и обеспечивающих защиту от угроз информационной безопасности;

29) **Информационно-коммуникационная инфраструктура платежной организации (далее – информационная инфраструктура)** – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним;

30) **Информационный актив платежной организации** – совокупность информации и объекта информационно-коммуникационной инфраструктуры, используемого для ее хранения и (или) обработки.

ГЛАВА 3. ОПИСАНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

3.1. Согласно учетной регистрации платежной организации, проведенной Национальным Банком Республики Казахстан, ТОО «Open Trade» оказывает следующие виды платежных услуг:

1) услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег;

2) услуги по реализации (распространению) электронных денег;

3) услуги по приему и обработке платежей, совершаемых с использованием электронных денег;

4) 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.

3.2. Услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег оказываются Платежной организацией в рамках договоров, заключаемых Платежной организацией с Получателями платежа – поставщиками Товаров, условиями которых предусмотрена возможность привлечения к оказанию платежных услуг платежных агентов/субагентов на основании отдельных агентских договоров по оказанию платежных услуг, заключаемых между Платежной организацией и платежным агентом, между платежными агентами и платежными субагентами (в случае привлечения платежного субагента).

Услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег оказываются путем приема от Клиента наличных денежных средств, внесенных через электронные терминалы (устройства), принадлежащие платежным агентам/субагентам, и последующего осуществления платежа без открытия банковского счета в пользу Получателя платежа.

3.3. Услуги по реализации (распространение) 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 (распространение) 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.

Отношения между эмитентом электронных денег и их владельцем - физическим лицом регулируются Законом о платежах и отдельным договором-офертой эмитента электронных денег по выпуску, использованию и погашению электронных денег, заключенным между ними в соответствии с законодательством Республики Казахстан. Договор-оферта эмитента электронных денег по выпуску, использованию и погашению электронных денег размещается на web-сайте эмитента в сети Интернет.

3.4. 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 «Open Trade», Оферта размещена на Сайте Системы.

3.5. Платежная 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 оказываются Платежной организацией на основании отдельных договоров, заключенных с банком/ банками второго уровня и платежной организацией с третьими лицами и обеспечивает прием платежей в электронных деньгах, 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 пользу соответствующего банка, а банк в свою очередь исполняет указание Клиента, переданное через Систему Платежной организации в электронной форме и перечисляет платеж бенефициару.

ГЛАВА 4. ПОРЯДОК И СРОКИ ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ КЛИЕНТАМ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ

4.1. Порядок оказания услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег.

Прием наличных денег для осуществления платежа без открытия банковского счета отправителя происходит путем внесения Клиентом денежных средств через электронный терминал (устройство) платежного агента/субагента (далее по тексту настоящего раздела Правил – «платежная услуга»). По факту внесения наличных денег, отправителю платежа выдается документ, подтверждающий платеж.

Оказание платежной услуги происходит в следующем порядке:

1) Платежный агент/субагент заключает с Платежной организацией (либо как с платежным агентом) договор об оказании платежных услуг.

2) Платежный агент/ субагент проходит регистрацию в Системе, с присвоением ему Платежной организацией персонального ID. Авторизация в Системе платежного агента/субагента с использованием персонального ID является идентификатором агента/субагента в Системе.

3) Оказание платежной услуги обеспечивается предоставлением платежным агентом/субагентом гарантийного взноса (авансового платежа) на планируемый объем платежей. Для этого платежный агент/субагент открывает расчетный счет в банке-партнере Платежной организации с функцией автосальдирования сумм, принятых платежей (по требованию агента\субагента Банком осуществляется автоматическое перечисление определенной суммы денег с текущего счета агента/субагента в течение согласованного с агентом/субагентом периода времени, в соответствии с требуемыми условиями). Сумма авансового платежа, внесенного платежным агентом/субагентом учитывается на его балансе в Системе. Платежный агент/субагент обязуется обеспечивать на вышеуказанном счете минимальный неснижаемый остаток денежных средств, достаточный для исполнения обязательств перед Платежной организацией и Клиентом по совершаемому платежу.

4) По факту совершения Клиентом платежа платежный агент/субагент в режиме реального времени передает в Систему данные о принятом платеже.

Платежный агент/субагент обязан передавать в Систему данные о каждом принятом платеже 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 Платежной организацией, подписанного присвоенным платежному агенту/субагенту ID в Системе.

5) Платежная организация по факту получения от платежного агента/субагента информации о Платеже, списывает с баланса платежного агента/субагента сумму в размере принятого платежа и зачисляет ее на лицевой счет – Получателя платежа.

При этом, в случае недостаточности на балансе платежного агента/субагента суммы гарантийного вноса для исполнения своих обязательств по принятому Платежу, такое обязательство платежного агента/субагента является необеспеченным, и Платежная организация вправе приостановить исполнение договора либо предоставить платежному агенту/субагенту отсрочку в перечислении платежа (коммерческий кредит, либо овердрафт) на основании отдельного соглашения заключаемого Платежной организацией с платежным агентом или гарантийного письма.

6) Платежный агент после приема платежа обязан выдать Клиенту квитанцию, подтверждающую использование электронного терминала (устройства) платежного агента/субагента для передачи данных о платеже.

7) При приеме платежей платежным агентом/субагентом взимается комиссия с платежа. Размер комиссии устанавливается платежным агентом/субагентом, и определяется условиями работы с Получателями – поставщиками Товаров.

8) Платежный агент/субагент обеспечивает размещение электронных терминалов по договору аренды с третьими лицами.

9) Всю информацию о статистике платежей, платежный агент/субагент получает на сайте <https://openpay.kz/>.

10) На ежемесячной основе платежный агент/субагент, предоставляет Платежной организации подписанный со своей стороны отчет платежного агента о принятых платежах, акт выполненных работ, счет-фактуру на сумму вознаграждения, на основании которого происходит сверка взаиморасчетов.

Сроки оказания платежных услуг – в течение 1 (одного) рабочего дня, следующего за днем приема платежа.

4.2. Порядок оказания услуги по реализации (распространение) 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 по реализации (распространению) электронных денег, выпущенных эмитентом в рамках системы электронных денег «Open Trade».

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 в следующем порядке:

Выпуск электронных денег осуществляется эмитентом электронных денег после получения денег от Клиента или агентов в сумме, равной номинальной стоимости принимаемых на себя обязательств.

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

Квитанция, содержит следующие реквизиты:

- 1) наименование и реквизиты эмитента, включая его бизнес-идентификационный номер;
- 2) время и дату совершения операции;
- 3) порядковый номер квитанции;
- 4) сумму принятых денег или поступивших платежей от владельца электронных денег;
- 5) сумму выпущенных электронных денег;
- 6) идентификационный код электронного кошелька владельца электронных денег-физического лица;
- 7) размер комиссионного вознаграждения (в случае взимания).

Допускается отражение в квитанции дополнительных реквизитов, установленных эмитентом электронных денег.

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

Сроки оказания платежной услуги – 1 (один) рабочий день с момента получения денег от физических лиц, электронные деньги реализуются физическому лицу с отражением в электронном кошельке владельца электронных денег.

4.3. 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 Системы, оператор системы электронных денег 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 в адрес эмитента электронных денег, распоряжения с использованием Электронных денег о совершении платежа в пользу конкретного Получателя платежа в электронном виде.

Для формирования распоряжения Клиент предоставляет реквизиты платежа (в том числе информации о: (i) Получателе платежа, в пользу которого осуществляется платеж с использованием электронных денег; (ii) платежных реквизитах, идентифицирующих назначение платежа (таких как номер и дата договора между Клиентом и Получателем платежа, иные реквизиты, в зависимости от того, какая информация подлежит предоставлению в момент совершения платежа); (iii) сумме платежа; и др.) одним из следующих способов:

- а) путем заполнения соответствующей формы на Сайте;

б) путем заполнения соответствующей формы на электронном терминале платежного агента/субагента;

в) путем заполнения соответствующей формы на мобильном устройстве с использованием мобильного приложения Системы ЭД.

Удостоверение распоряжения на совершение платежа производится в зависимости от настроек Системы ЭД, установленных самим Клиентом:

- путем ввода Клиентом Аутентификационных данных, присвоенных ему в момент регистрации Учетной записи Клиента;
- путем ввода Клиентом Аутентификационных данных, присвоенных ему в момент регистрации Учетной записи Клиента, а также введения Кода подтверждения, отправленного/переданного на Абонентский номер программными средствами Платежной организации;
- путем использования команд посредством Message-подтверждения платежей.

Ввод корректных Аутентификационных данных, Кодов подтверждения, либо команд посредством Message-подтверждения платежей признается сторонами в качестве однозначного и бесспорного подтверждения совершенных платежей.

Использование Аутентификационных данных в электронных сообщениях, передаваемых Клиентом в целях авторизации Учетной записи и использования Системы ЭД, Кодов подтверждения, команд, переданных посредством Message-подтверждения в целях формирования и направления распоряжений, порождает юридические последствия, аналогичные использованию собственноручных подписей в соответствии с требованиями законодательства Республики Казахстан, а все документы, связанные с исполнением Договора на оказание услуг, заключенного на условиях Оферты, и удостоверенные любым из вышеизложенных способов, признаются документами в письменной форме.

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 «Open Trade».

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 Учетной записи Клиента, доступ к которой предоставлен Клиенту на Сайте Системы. Клиент обязуется проверять информацию не менее 1 (одного) раза в день. В случае если Клиент не проверяет информацию о совершении платежей 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 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.

4.3.1. Регистрация в Системе электронных денег «Open Trade» Партнеров, принимающих к оплате электронные деньги:

Для принятия к оплате юридическим лицом и/или индивидуальным предпринимателем (далее – «Партнер») 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 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.

4.3.2. Порядок формирования статистической и иной отчетности для эмитента электронных денег

Платежная организация ежедневно передает Эмитенту следующий набор входящих файлов и отчетов, содержащих информацию о совершенных операциях с электронными деньгами:

1) Входящие файлы (реестры), предназначенные для автоматизированного учёта операций:

- файл детализовки операций, проведенных в Системе ЭД;
- файл сводных сумм по контрагентам с детализовкой по коду провайдера/агента;
- файл сводных сумм по контрагентам - результат группировки файла детализовки операций по коду операции и ID контракта;
- файл платежных поручений, оформленных Клиентами через Сайт Системы или электронные терминалы платежных агентов/субагентов;
- файл сводных платежных поручений, сформированных посредством группировки платежных поручений, оформленных Клиентами; файл оборотов и остатков по кошелькам;

2) Отчеты:

- отчет по расчетам с контрагентами по операциям оплаты товаров и услуг и пополнениям кошелька в человеко-читаемом формате (повторяет содержимое файла сводных сумм по контрагентам). отчет по сводным платежным поручениям (погашениям кредитов) в человеко-читаемом формате (повторяет содержимое файла сводных платежных поручений);
- отчет по остаткам и оборотам по кошелькам.

Так же на ежемесячной и ежеквартальной основе формируется и передается отчет для Национального Банка Республики Казахстан, формируемый в соответствии с

установленными нормативными правовыми актами Национального банка Республики Казахстан.

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

Согласно нижеприведенной схеме – движения денежных и информационных потоков между участниками Системы ЭД, выпуск (эмиссия) электронных денег (эмиссия) осуществляется Эмитентом после получения денег от Клиентов, при условии регистрации в Системе ЭД в соответствии с Правилами.

Выпуск электронных денег Клиенту осуществляется Эмитентом после внесения Клиентом платежа следующим образом:

- 1) Безналичный перевод денег;
- 2) Внос наличных денег.

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

Приобретение Партнером у Эмитента электронных денег осуществляется путем безналичного перевода денег на банковский счет Эмитента, с указанием номера пополняемого Электронного кошелька и указанием цели перевода.

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

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

Электронные деньги Клиента и/или Партнера 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/Партнера.

4.3.4. Порядок погашения электронных денег для идентифицированных/не идентифицированных владельцев электронных денег.

Погашение электронных денег — платежная услуга, предусматривающая осуществление Эмитентом обмена выпущенных им электронных денег, предъявленных Клиентами/ Партнерами, либо подлежащих обмену без их предъявления владельцем в случаях, предусмотренных законами Республики Казахстан, на равную по их номинальной стоимости сумму 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.

Погашение электронных денег для идентифицированного владельца электронных денег на банковский счет владельца электронных 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.

1) в случае, если при проверке Эмитентом данных, указанных владельцем электронных денег/клиентом в указании, банковский счет принадлежит клиенту – операция считается успешной и эмитент осуществляет гашение электронных денег на банковский счет клиента;

2) в случае, если при проверке эмитентом данных, указанных клиентом в указании, банковский счет не принадлежит Клиенту - погашение электронных денег не производится. Клиенту направляется уведомление о незавершенной операции по погашению электронных денег в связи с несовпадением идентификационных данных владельца электронных денег и владельца банковского счета.

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

Погашение электронных денег через кассу эмитента осуществляется на момент предъявления указания о погашении электронных денег при личном присутствии в отделении/филиале Эмитента путем заполнения Клиентом заявления на погашение электронных денег по форме, установленной Эмитентом, с предоставлением Эмитенту документа, удостоверяющего личность, с индивидуальным идентификационным номером(ИИН) и абонентского договора между Клиентом и оператором мобильной связи о предоставлении услуг связи.

Эмитент осуществляет сверку полученных данных, а также отправляет сообщение Платежной организации о погашении электронных денег по данному заявлению Клиента.

При погашении электронных денег сумма выдаваемых денег должна соответствовать сумме электронных денег, предъявленных к погашению.

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 учредительных документов, бизнес-идентификационный номер, а также адрес места нахождения;

4.3.5. Порядок закрытия электронного кошелька в системе электронных денег.

1) Закрытие Электронного кошелька Партнером.

При закрытии Электронного кошелька Партнер уведомляет Платежную организацию о намерении закрыть такой Электронный кошелек. Платежная организация формирует дополнительное соглашение о расторжении договора по согласию сторон, содержащее указание Партнера о сроке и порядке погашения электронных денег, находящихся на Электронном кошельке.

После подписания сторонами дополнительного соглашения о расторжении договора Платежная организация направляет Эмитенту указание Партнера о закрытии Электронного кошелька для перевода остатка неизрасходованных электронных денег на его банковский счет.

2) Закрытие электронного кошелька Клиента – физического лица.

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) в наличной и/или безналичной форме. В случае, если Клиент неидентифицирован, для закрытия Электронного кошелька ему необходимо пройти процедуру идентификации. После прохождения такой процедуры (если Клиент не был идентифицирован) Клиент отправляет указание о закрытии Электронного кошелька и о выводе электронных денег способами, указанными выше. После погашения электронных денег Платежная 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.

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

4.4. 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.

В рамках исполнения/оказания данной услуги Платежная организация обеспечивает:

1) Прием информации о платежах, инициированных Клиентом с использованием платежных карточек с указанием реквизитов назначения соответствующего платежа и бенефициара с последующим обеспечением передачи реквизитов по платежу для его исполнения в пользу 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 посредством программного обеспечения, обеспечивающего возможность инициации клиентом в электронной форме распоряжений на списание денег с платежной карточки/банковского счета клиента, с целью последующего исполнения поручения/ распоряжения клиента,

полученного Платежной организацией от Клиента и переданного Платежной организацией в Банк.

3) При оказании услуги Платежная организация обеспечивает следующий алгоритм действий при обработке платежей:

- Клиент посредством сети интернет/ мобильного телефона заходит на платежную форму Платежной организации;
- Клиент знакомится с тарифом/ размером комиссии за предоставление Платежной организацией соответствующей услуги;
- Клиент знакомится с условиями предоставления услуги и соглашается с условиями договора- оферты, размещенными в соответствующем разделе;
- Клиент на платежной странице инициирует платеж в пользу Мерчанта;
- Мерчант, по согласованию с Платежной организацией, выбирает наиболее удобный для себя вариант Авторизации (однотактный либо двухтактный);
- Клиент вводит в платежную форму реквизиты для исполнения платежа Банком;
- Для совершения платежа клиент вводит реквизиты Платежной карточки, банковского счета;
- Платежная организация посредством запроса в Банк инициирует исполнение распоряжения клиента, полученного в электронной форме;
- Банк, получив подтверждение от Платежной организации и клиента производит списание денег с Платежной карточки/банковского счета, и перевод Платежа в пользу Поставщика услуг, указанного в поручении Клиента, суммы инициируемой клиентом операции с учетом вознаграждения Платежной организации и комиссионного вознаграждения Платежной организации.
- Платежная организация получает от Банка подтверждение исполнения Операции;
- Платежная организация выдает клиенту электронный чек, подтверждающий совершение клиентом операции и списание с клиента комиссии Платежной организации.

Платеж считается принятым и становится окончательным с момента направления Клиенту подтверждения о приеме Платежа (квитанция об оплате).

В случае возврата/отказа Клиентом от платежной услуги, либо необходимости проведения отмены ранее осуществленной Операции оплаты, Мерчант инициирует проведение таких операций в личном кабинете Системы.

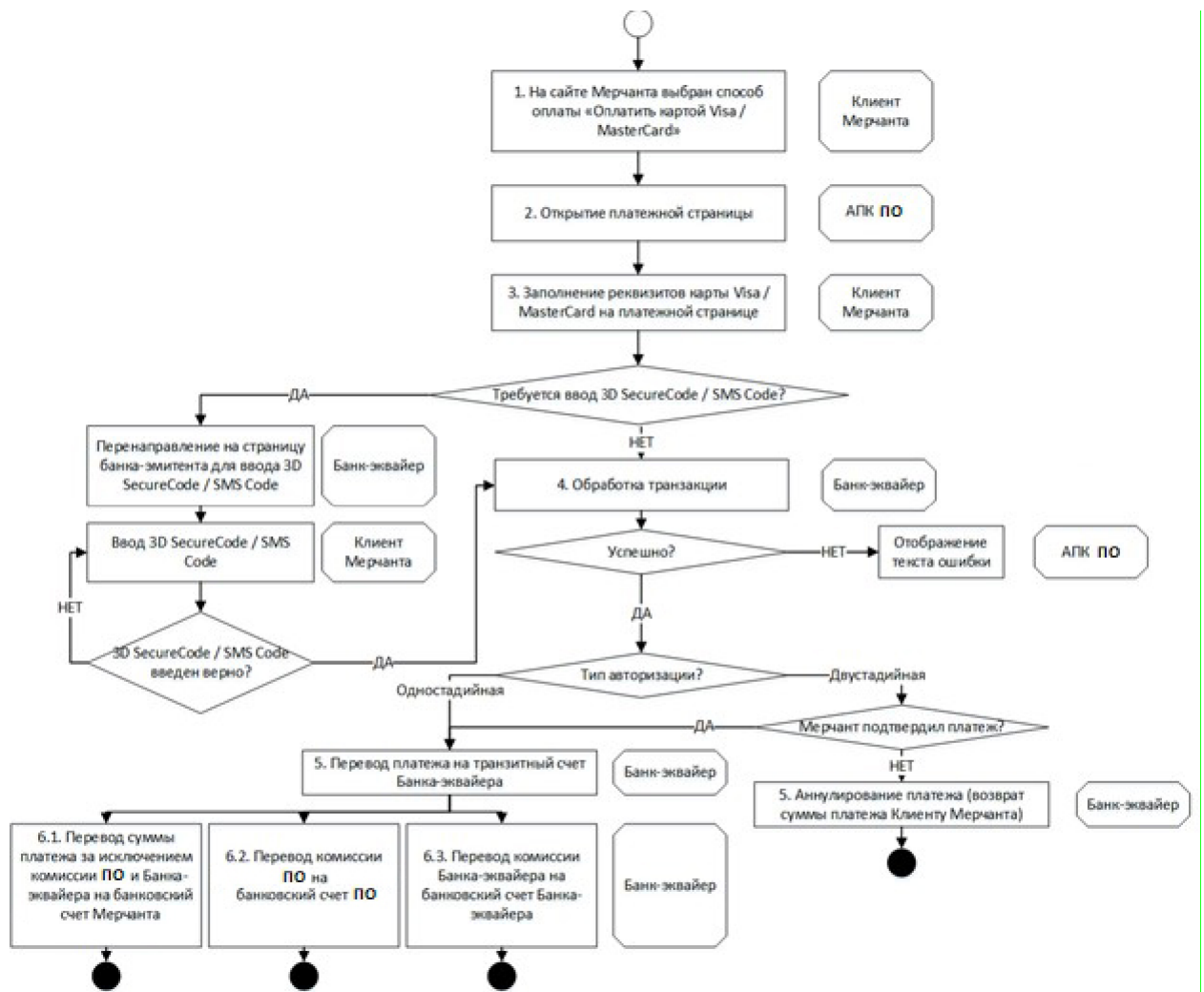
Фиксация совершения операций осуществляется Платежной организацией в электронном виде и хранится в АПК Платежной организации. Выписки из АПК Платежной организации могут использоваться в качестве доказательств при рассмотрении споров, в том числе в судебном порядке.

По результатам обработки Операций Платежная организация направляет Мерчанту отчет по успешно прошедшим транзакциям.

Перевод денег осуществляется со счета Банка-эквайера на счет Мерчанта, за исключением вознаграждения Платежной организации и комиссии Банка-эквайера или со счета Банка – эквайера на специальный (транзитный) счет Банка, с которым у Платежной организации заключен соответствующий договор. После зачисления платежей на специальный (транзитный) счет Банка, Платежная организация передает в электронном виде Банку реестры платежей с указанием суммы и реквизитов Мерчанта, которому

необходимо зачислить платежи, после чего Банк осуществляет перевод платежей на счет Мерчанта. Детальная схема приведена на рисунке 1.

Рисунок 1



4.1.2. Детализированное описание передвижения денег при положительно обработанной операции оплаты:

1. Банк-эмитент осуществляет списание денег с карты Клиента;
2. Банк-эмитент осуществляет платеж в пользу Банка-эквайера;
3. Банк-эквайер перечисляет платеж на счет Мерчанта.

4.1.3. Платежная организация осуществляет следующие действия при оказании платежной услуги и осуществлении Процессинга при переводе денег на платежную карточку:

- Платежная организация в ежедневном круглосуточном режиме реального времени принимает запросы на переводы от Клиента;
- По факту получения такого запроса и при условии возможности оказания услуги в соответствии Правилами МПС Платежная организация передает Банку, с которым у платежной организации заключен соответствующий договор, информацию о списании денег с отправителя и зачислении денег на платежную карточку получателя;
- Банк, по получению информации от Платежной организации, являясь оператором по переводам, осуществляет перевод на платежную карточку получателя перевода;
- Платежная организация осуществляет обработку операций, в сроки и в соответствии с Правилами Платёжной Системы;
- Платежная организация в режиме реального времени информирует Клиента о результате оказания услуги в отношении каждой конкретной операции.

4.1.4. Подтверждение оказания платежной услуги Покупателю

В качестве подтверждения оказания платежной услуги Клиенту, Платежная организация посредством Системы формирует и направляет Клиенту квитанцию, в электронном виде, на электронный адрес Клиента или путем SMS сообщения на номер телефона Клиента. Квитанция в обязательном порядке должна содержать информацию, установленную Законом о платежах и Правилами № 215. Допускается проставление Платежной организацией в документе, подтверждающем факт оказания платежной услуги, дополнительных реквизитов по оказанной платежной услуге.

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

ГЛАВА 5. СТОИМОСТЬ ПЛАТЕЖНЫХ УСЛУГ (ТАРИФЫ), ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

Тарифы платежной организации ТОО «Open Trade» по платежным услугам:

1. Услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег:

№	Наименование категорий сервисов, предоставляемых Поставщиками услуг	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента.
1.	Игровые сервисы	от 0 % до 25% от суммы операции
2.	Электронные деньги	от 0 % до 5% от суммы операции

3.	Букмекеры	от 0 % до 25% от суммы операции
4.	Социальные сети	от 0 % до 15% от суммы операции
5.	Сотовые операторы	от 0 % до 5% от суммы операции
6.	Подарочные карты, купоны	от 0 % до 10% от суммы операции
7.	ЖКХ	от 0 % до 5% от суммы операции
8.	MLM	от 0 % до 10% от суммы операции
9.	Интернет и телефония	от 0 % до 5% от суммы операции
10.	Хостинг	от 0 % до 10% от суммы операции
11.	Благотворительность	Не взимается
12.	Реклама	от 0 % до 15% от суммы операции
13.	Страхование	Не взимается
14.	Интернет - магазины	от 0 % до 15% от суммы операции
15.	Билеты (авиа, ж/д)	от 0 % до 10% от суммы операции
16.	МКО	от 0 % до 15% от суммы операции
17.	Прочие виды сервисов, не включенные в отдельные категории	от 0 % до 20% от суммы операции

2. Услуги по реализации (распространению) электронных денег:

№	Категория сервиса	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента.
1.	Реализация (распространение) ЭД:	от 0 % до 5% от суммы реализованных электронных денег

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

№	Категория сервиса	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента.
---	-------------------	--

1.	Приему и обработка платежей, совершаемых с использованием электронных денег в системе электронных денег «Open Trade»:	от 0 % до 5% от суммы принятых и обработанных электронных денег
2.	Предоставление неактивному пользователю использование системы электронных денег «Open Trade»	50 (пятьдесят) тенге за 1 (один) календарный день
3.	Закрытие электронного кошелька Клиента в системе электронных денег «Open Trade».	0%

4. 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	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента.
1.	Игровые сервисы	от 0 % до 25% от суммы операции
2.	Электронные деньги	от 0 % до 5% от суммы операции
3.	Букмекеры	от 0 % до 25% от суммы операции
4.	Социальные сети	от 0 % до 15% от суммы операции
5.	Сотовые операторы	от 0 % до 5% от суммы операции
6.	Подарочные карты, купоны	от 0 % до 10% от суммы операции
7.	ЖКХ	от 0 % до 5% от суммы операции
8.	MLM	от 0 % до 10% от суммы операции
9.	Интернет и телефония	от 0 % до 5% от суммы операции
10.	Хостинг	от 0 % до 10% от суммы операции
11.	Благотворительность	Не взимается
12.	Реклама	от 0 % до 15% от суммы операции
13.	Страхование	Не взимается
14.	Интернет - магазины	от 0 % до 15% от суммы операции

15.	Билеты (авиа, ж/д)	от 0 % до 10% от суммы операции
16.	МКО	от 0 % до 15% от суммы операции
17.	Прочие виды сервисов, не включенные в отдельные категории	от 0 % до 20% от суммы операции

- Стоимость дополнительной платы (допустимой дополнительной комиссии) взимаемой с Клиента устанавливается в соответствии с договорными условиями, указанными в договорах, заключенных между ТОО «Open Trade» и поставщиками услуг, эмитентами электронных и иными лицами, предоставляющими услуги Клиентам.

- Ценовая политика по взимаемой дополнительной комиссии с плательщика устанавливается Платежной организацией самостоятельно в рамках допустимых значений, указываемых в договорах.

- Дифференциация процентного соотношения допустимой дополнительной комиссии, взимаемой с плательщика, зависит от рыночных условий по каждому сервису.

Приведенный выше список сервисов не является исчерпывающим и может дополняться по мере заключения новых договоров с поставщиками услуг.

ГЛАВА 6. ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ТРЕТЬИМИ ЛИЦАМИ, ОБЕСПЕЧИВАЮЩИМИ ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

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

- предоставляют услуги платежной организации или действуют в интересах платежной организации;
- не входят в группу компаний 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 или договоров поручения на прием платежей, которые обязательно включают в себя пункты 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.

Платежная организация, с соблюдением всех требований и норм Закона о платежах, имеет право передать третьим лицам на основании договора о возмездном оказании услуг исполнения информационно-технологических функций, необходимых для обеспечения оказания платежных услуг Платежной организацией (договор об аутсорсинге), при этом Платежная организация имеет право заключить лицензионный договор, в котором будут описаны информационно-технологические функции, осуществляемые третьими лицами, необходимые для обеспечения оказания платежных услуг Платежной организацией.

6.2. Порядок взаимодействия Платежной организации и Поставщиком услуг.

6.2.1. Платежная организация заключает с Поставщиком услуг договор об оказании платежных услуг, который должен содержать следующую информацию:

- виды и общая характеристика оказываемых платежных услуг;
- порядок и максимальный срок оказания платежной услуги;
- размеры взимаемых сборов и комиссий или указание интернет-ресурса, содержащего данную информацию, и порядок их взимания;
- порядок предоставления информации о платежной услуге;
- порядок защитных действий от несанкционированных платежей;
- порядок определения обменного курса, применяемого при оказании платежной услуги в иностранной валюте;
- условия, при которых платежная организация оставляет за собой право на отказ в оказании платежной услуги;
- порядок регулирования вопросов по несанкционированным платежным услугам;
- право Мерчанта на расторжение договора;
- порядок предъявления претензий и разрешения спорных ситуаций;
- порядок и размеры выплат по возмещению ущерба за необоснованный отказ от исполнения либо ненадлежащее исполнение указания.
- Платежной организацией могут быть предусмотрены дополнительные условия, необходимые при оказании платежной услуги.

6.2.2. Поставщик услуг проходит регистрацию в Системе Платежной организации, с присвоением ID, для чего:

- В согласованный сторонами договора срок Поставщик услуг осуществляет реализацию Интерфейса подключения (API) к Системе Платежной организации.
- Стороны проводят техническое тестирование систем;
- Сторонами определяется техническая готовность систем к отправке информации о платежах.
- Платежная организация обязана передавать данные Мерчанту о каждом обработанном платеже для внесения изменений в лицевой счет Клиента Мерчантом. Сведения должны быть переданы непосредственно в период обработки платежа на основании данных, указываемых физическим лицом, без ошибок и искажений.

- Каждой операции по передаче данных о платеже присваивается уникальный номер в Системе Платежной организации.
- Платежная организация с Мерчантом проводит ежедневную сверку по успешно обработанным платежам.
- На ежемесячной основе производится сверка взаиморасчетов.

6.3 Порядок взаимодействия Платежной организации и Банком.

6.3.1. Платежная организация заключает с Банком договор о взаиморасчетах и информационно-техническом взаимодействии, который должен содержать следующую информацию:

- виды и общая характеристика оказываемых услуг;
 - порядок и максимальный срок оказания услуг;
 - размеры взимаемых сборов и комиссий, и порядок их взимания;
 - порядок предоставления информации о Мерчанте;
 - условия, при которых Банк оставляет за собой право на отказ в оказании услуг;
 - порядок предъявления претензий и разрешения спорных ситуаций;
 - финансовые условия и порядок расчетов с Платежной организацией и Мерчантом.
- Банком могут быть предусмотрены дополнительные условия, необходимые при оказании услуг.

6.3.2. 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 передает данные Банку о каждом обработанном платеже.
- Банк передает Платежной организации данные о каждом успешно 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 успешно обработанным платежам.
- На ежемесячной основе производится сверка взаиморасчетов.

6.4. Порядок взаимодействия Платежной организации с Платежным агентом.

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

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

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

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

6.4.5. При отсутствии в день приема платежей денежных средств в остатке гарантийного вноса 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.

6.4.6. 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.

6.4.7. Каждая операция по передаче данных о платеже сопровождается подписанием платежным агентом/субагентом электронного документа, форма которого согласована с соответствующим Платежной организацией. 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.

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

**Все договоры заключенные Платежной организацией должны соответствовать действующему законодательству Республики Казахстан.*

ГЛАВА 7. СВЕДЕНИЯ О СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ, ИСПОЛЬЗУЕМОЙ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

Система управления рисками направлена на обеспечение финансовой устойчивости и стабильного функционирования Платежной организации, представляет собой систему организации, политик, процедур и методов, принятых Платежной организацией с целью своевременного выявления, измерения, контроля и мониторинга рисков Платежной организации для обеспечения её финансовой устойчивости, и стабильного функционирования.

Платежная организация в целях эффективного управления рисками разработала политику управления рисками, которая 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 этих целях в Платежной организации закреплен работник (в случае отсутствия такого работника, данные функции выполняет Директор), 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.

По договорам с платежными агентами в целях предотвращения финансовых рисков используется обеспечительный взнос, выплачиваемый Платежной организации платежным агентом по договору, в объеме необходимом для приема платежей. В случае, если сумма обеспечительного взноса исчерпана, то система автоматически блокирует прием платежей.

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

- размер, характер и сложность бизнеса;
- доступность рыночных данных для использования в качестве исходной информации;
- состояние информационных систем и их возможности;
- 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:

- определение организационной структуры управления рисками, обеспечивающей контроль за выполнением партнерами Платежной организации требований к управлению рисками, установленных правилами управления рисками Платежной организации;
- определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;
- доведение до органов управления Платежной организации соответствующей информации о рисках;
- определение показателей бесперебойности функционирования Системы Платежной организации;
- определение порядка обеспечения бесперебойности функционирования Системы Платежной организации;
- определение методик анализа рисков;
- определение порядка обмена информацией, необходимой для управления рисками;
- определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев; определение порядка изменения операционных и технологических средств и процедур;
- определение порядка оценки качества функционирования операционных и технологических средств, информационных систем;
- 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:

- установление предельных размеров (лимитов) обязательств Мерчантов;
- установление предельных размеров (лимитов) обязательств агентов и субагентов Платежной организации с учетом уровня риска;
- установление обеспечительного взноса агентов и субагентов Платежной организации в рамках оказываемых платежных услуг;
- управление очередностью исполнения распоряжений должностными лицами;
- осуществление расчета в платежной организации до конца рабочего дня;
- обеспечение возможности предоставления лимита;
- использование безотзывных банковских гарантий;
- другие способы управления рисками.

ГЛАВА 8. ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ И РАЗРЕШЕНИЯ СПОРОВ С КЛИЕНТАМИ (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.

Клиенту необходимо обратиться к Платежной организации с письменным заявлением, составленным в произвольной форме, содержащим указание на возникшую спорную ситуацию (далее – «Претензия»), одним из следующих способов:

1. путем направления его почтовым отправлением по адресу – Республика Казахстан, город Алматы, Бостандыкский район, Микрорайон Архат улица 7, дом, 19;
2. путем личного обращения в офис Платежной организации и ее нарочным предоставлением по адресу: Республика Казахстан, город Алматы, Бостандыкский район, Микрорайон Архат улица 7, дом, 19.

При каждом из перечисленных способов направления Платежной организации Претензии Клиента, она подлежит регистрации Платежной организацией путем присвоения даты и порядкового номера входящей корреспонденции. Датой приема Претензии Клиента Платежной организацией считается фактическая дата регистрации входящего обращения Клиента.

Обращения в службу технической поддержки плательщиков по телефону, направления сообщений через форму обратной связи на WEB-сайте 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).

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

Для надлежащего рассмотрения Претензии Клиента и подготовки ответа платежная организация:

- 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);

- запрашивает и получает от Клиента дополнительно документы (или их копии), объяснения и иные сведения. По запросу платежной организации плательщик обязан предоставить запрашиваемые платежной организацией сведения и документы (их копии) в целях надлежащего досудебного урегулирования возникшего спора;

- проводит тщательный анализ полученных сведений и разъяснений для формирования полного и достоверного ответа на Претензию Клиента;

- 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.

ГЛАВА 9. ПОРЯДОК СОБЛЮДЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В Платежной организации реализована и функционирует система управления информационной безопасности (СУИБ).

Целью СУИБ является обеспечение бесперебойной работы Платежной организации, конфиденциальности, целостности и доступности информации, сведение к минимуму ущерба от событий, таящих угрозу информационной безопасности, посредством предотвращения таких событий и сведения их последствий к минимуму.

СУИБ распространяется на все информационные активы Платежной организации, перечисленные в перечне защищаемых информационных активов, и пересматривается при изменении перечня или изменении значимости защищаемых информационных активов.

Для достижения своей цели СУИБ реализуется в рамках циклической модели управления и состоит из процессов планирования, реализации, проверки и совершенствования.

В рамках планирования деятельности по обеспечению информационной безопасности осуществляются следующие процессы:

- устанавливаются цели, задачи, процессы и процедуры, адекватные потребностям в управлении рисками информационной безопасности и совершенствовании СУИБ;

- проводится идентификация информационных активов;

- разрабатывается модель угроз и нарушителей;

- разрабатываются меры защиты информационных активов от актуальных угроз.

В рамках реализации деятельности по обеспечению информационной безопасности осуществляются следующие процессы:

- Гарантирование использования по назначению компьютеров и телекоммуникационных ресурсов Компании ее сотрудниками, независимыми подрядчиками и другими пользователями;
- выявления, реагирования (противодействие атакам в реальном времени), разрешения и анализ причин возникновения инцидентов информационной безопасности;
- управления доступом к активам;
- антивирусной защиты;
- резервного копирования активов;
- управления непрерывностью бизнеса;
- регистрации, анализа и контроля событий информационной безопасности;
- выявление уязвимостей в информационных системах платежной организации, с использованием которых могут быть реализованы угрозы информационной безопасности;
- формирования принципов внесения изменений, процедуры установки, модификации и технического обслуживания информационных систем платежной организации;
- физической безопасности активов;
- защита сетевого периметра;
- соблюдение условий всех программных лицензий, авторских прав и законов, касающихся интеллектуальной собственности;
- обучение персонала.

На стадии проверки осуществляется оценка, измерение эффективности процессов СУИБ на соответствие целям и установленным практикам, обеспечивается отчетность руководству Платежной организации о результатах для проведения соответствующего анализа.

На стадии совершенствования осуществляются выработка и принятие корректирующих и превентивных действий, основанных на результатах анализа, для достижения непрерывного совершенствования СУИБ Платежной организации.

Идентификация информационных активов, определение их ценностей

Разработка и поддержание успешной СУИБ основывается на идентификации информационных активов. Результатом идентификации является формирование структурированного по типам перечня защищаемых активов с указанием их ценности. При идентификации ИА выделяется информация ограниченного доступа (платежная информация, коммерческая тайна, персональные данные и пр.) и общедоступная информация.

Инвентаризация информационных активов производится на плановой основе 1 раз в год.

При введении новой бизнес-услуги (продукта), а также при существенном изменении уже существующих бизнес-услуг, производится анализ информационных активов с целью определения необходимости дополнения перечня защищаемых активов.

Управление рисками информационной безопасности

Информационные активы подвержены многим угрозам.

Главный инструмент СУИБ – основанный на опыте, в том числе, опубликованном в открытых средствах массовой информации или сети Интернет, прогноз вероятных сценариев реализации угроз.

Как оценка уязвимостей информационных активов, так и оценка рисков информационной безопасности производится только на основе рассмотрения конкретного сценария модели угроз. Так как с течением времени угрозы, их источники и риски могут изменяться, модели угроз и нарушителей периодически пересматриваются.

Для противодействия угрозам информационной безопасности Платежная организация придерживается принципа сбалансированности реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Платежной организации до специализированных мер информационной безопасности по каждому выявленному риску, основанных на оценке рисков.

При оценке рисков информационной безопасности используется модель угроз и нарушителей, учитывается ценность информационных активов, степень актуальности угроз информационной безопасности и степени уязвимости информационных активов.

Оценка рисков должна проводиться не реже 1 раза в год, а также при любых изменениях в перечне защищаемых информационных активов.

Обнаружение и реагирование на инциденты информационной безопасности

Каждый сотрудник Платежной организации отвечает за соблюдение информационной безопасности на своем рабочем месте.

Обнаружение сотрудниками Платежной организации событий и слабых мест информационной безопасности, связанных с информационными системами, гарантирует возможность принятия своевременных корректирующих действий.

В Платежной организации разработан Регламент, обеспечивающие незамедлительное реагирование сотрудников в случае обнаружения инцидента информационной безопасности.

Все обнаруженные инциденты информационной безопасности регистрируются и расследуются с целью определения причин их возникновения и предотвращения их повторения. Уязвимости информационной безопасности, обнаруженные при выполнении мероприятий мониторинга, подлежат учету с целью дальнейшего планирования действий по их устранению.

На каждый инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности. Все инциденты информационной безопасности регистрируются в Журнале учета.

Срок хранения информации об инцидентах информационной безопасности составляет 5 лет.

В срок до 48 часов Платежная организация уведомляет Национальный Банк об инцидентах информационной безопасности:

- 1) эксплуатация уязвимостей в прикладном и системном программном обеспечении;
- 2) несанкционированный доступ в информационную систему;
- 3) атака "отказ в обслуживании" на информационную систему или сеть передачи данных;
- 4) заражение сервера вредоносной программой или кодом;
- 5) совершение несанкционированного перевода денежных средств вследствие нарушения контролей информационной безопасности;
- 6) инцидентах информационной безопасности, несущих угрозу стабильности деятельности платежной организации.

Информация предоставляется в виде карты инцидента информационной безопасности, по форме установленной Национальным банком.

Информация по обработанным инцидентам информационной безопасности представляется в электронном формате с использованием платформы Национального Банка для обмена событиями и инцидентами информационной безопасности.

Обеспечение безопасности вычислительных сетей.

Защита сетевой инфраструктуры платежной организации является одной из основных задач обеспечения информационной безопасности. Вся информационная инфраструктура платежной организации является средой обработки критичных данных. Принимая во внимание то, что основные бизнес-функции, связанные с обработкой данных, реализуются при помощи связанных вычислительной сетью компонентов информационной инфраструктуры, защита от сетевых угроз является приоритетным направлением обеспечения информационной безопасности.

Сервер

Доступ до терминальной сессии сервера осуществляется путём аутентификации. Одновременно допускается использовать максимум 2 сессии терминала.

Рабочие станции

Доступ в интернет рабочих станций осуществляется путём подключения к Wifi роутеру с защитой подключения типа WPA2-PSK. Все рабочие станции должны быть подключены только к локальной сети платежной организации. Контроль ограничений входящих и исходящих подключений осуществляется путём настройки межсетевого экрана. Доступ к рабочим станциям осуществляется путём аутентификации пользователя учётной записью домена Active Directory. Пароль от учетной записи выдаётся работнику под личную ответственность для доступа к своей рабочей станции. Пароль может быть изменен Системным Администратором.

Управление доступом пользователей к данным

Доступ пользователей к данным является фактором риска информационной безопасности. Процесс управления доступом регламентирован в Платежной организации. Предоставление доступа пользователей к данным осуществляется в соответствии с принципом минимально необходимых привилегий для осуществления должностных обязанностей. Также в Платежной организации реализована и поддерживается система управления парольными политиками.

Управление учётными записями и парольной защиты

Работа пользователей в ОС и ИС осуществляется под уникальными учетными записями. Каждому пользователю назначается сертификат для двухфакторной авторизации.

Не допускается работа пользователя под чужой учетной записью и учетной записью «Администратор», а также включение пользователя в привилегированную группу «Администраторы». Учетная запись «Гость» в операционной системе должна быть отключена. Аутентификация на сервере осуществляется путём подключения к терминалу и ввода пользователем персональных данных, созданных Системным администратором. Для предоставления временного доступа к ресурсам Платежной организации (для лиц, не

являющихся работниками Платежной организации, для работников, которым необходимо получить временный доступ к ресурсам Платежной организации, и т.п.) необходимо использовать временные учетные записи (с фиксированным сроком действия) в ОС.

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.

Пароли учетных записей в ОС и ИС. Пароли оборудования

Пароль учетных записей ОС и ИС должен иметь длину не менее 8 символов для пользователей и привилегированных пользователей, а также для служебной, системной, встроенной или технологической учетной записи. Пароль пользователей должен быть достаточно сложным и содержать в себе как минимум комбинацию прописных и заглавных букв, цифр. Также возможно, но не обязательно использование специальных символов. Пароль привилегированных пользователей, а также для служебной, системной, встроенной или технологической учетной записи должен содержать в себе символы всех четырех категорий: буквы нижнего регистра, буквы верхнего регистра, цифры и специальные символы (@, #, \$, &, *, % и т.п.). Пароли учетных записей ОС и ИС должны изменяться: для систем, которые поддерживают автоматическую смену паролей, смена пароля осуществляется ежемесячно (каждые 30 дней), а системы, которые не поддерживают автоматическую смену пароля, смена пароля осуществляется каждые 3 месяца (90 дней), исключением является SQL, в которой пароль меняется только в том случае, если работник забыл ранее выданный пароль. Пароли на оборудовании (маршрутизаторы, коммутаторы, беспроводные точки доступа, офисная мини-АТС, видеорегистраторы и др.) должны меняться Системным администратором каждые 180 дней. При смене пароля новый пароль не должен повторять ни один из 12 последних использованных данным пользователем паролей. Данное требование не относится к ИС, в которых не реализована данная функция. Пароль не должен включать в себя осмысленные слова, словосочетания, общепринятые аббревиатуры, а также легко идентифицируемую с его владельцем информацию – имена, фамилии, названия учетных записей, номера телефонов, клички животных, наименования организаций и т.п. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименование автоматизированного рабочего места - АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

Встроенные учетные записи

Пароли, установленные по умолчанию производителем ИС для встроенных учетных записей, должны быть изменены при вводе ИС в эксплуатацию. Это относится и к любому серверному и коммуникационному оборудованию, если это технически возможно. Категорически запрещается использование встроенных учетных записей Administrator (SA для 1С и SQL сервера, root в Unix и т.п.) - для повседневной работы, для запуска служб и сервисов либо для доступа к сетевым ресурсам. Использование встроенных учетных записей допускается только в случаях, требующих реквизитов именно этой учетной записи (восстановление ОС, восстановление поврежденных данных системы, в некоторых случаях проведение обновлений системы и т.п.). Для встроенных учетных записей Administrator должно быть включено логирование всех действий. Все неиспользуемые учетные записи должны быть отключены или удалены

При увольнении работника

При увольнении работника его учётная запись удаляется/отключается. При выходе работника в любой вид отпуска, а также на больничный, учетные записи в ОС и ИС должны быть заблокированы до момента выхода на работу. Пользователям запрещается разглашать информацию о своих учетных записях. Пользователям запрещается предоставлять доступ к своей учетной записи другим работникам Компании или третьим лицам. В случае служебной необходимости, разрешается работать на персональном компьютере другого работника платежной под своей учетной записью с устного разрешения его непосредственного руководителя. Исключением является исполнение своих должностных обязанностей Системным администратором при настройке компьютера/ноутбука пользователя по поданной заявке на бумажном носителе. В этом случае, Системный администратор может производить исполнение заявки и в отсутствие пользователя, но в этом случае, после выполнения всех работ, Системный администратор обязан выключить компьютер пользователя (если пользователь так и не пришел на свое рабочее место). При уходе в отпуск или при переводе работника в другое подразделение, работник должен позаботиться о передаче необходимой информации заменяющему его лицу, а непосредственный руководитель должен проконтролировать данный процесс. При отсутствии пользователя в течение 5 минут на рабочем месте (неактивное состояние компьютера), компьютер должен быть автоматически переведен в заблокированное паролем состояние. Блокировка выполняется путем настроек ОС на рабочей станции работника. Помимо этого, каждый работник Компании, уходя с рабочего места обязан самостоятельно заблокировать свою учетную запись, нажав на клавиатуре комбинацию клавиш «эмблема Windows+L», либо «CTRL+ALT+DELETE» и затем нажать «Блокировать компьютер».

Привилегированные учетные записи

Под привилегиями понимаются идентификаторы, созданные для выполнения таких служебных задач, как администрирование приложений, баз данных, серверов, операционных систем и т.д.

Привилегии должны назначаться для пользовательских идентификаторов, не совпадающих с теми, что применяются для обычной деловой деятельности.

Доступ к привилегиям предоставляется уполномоченным сотрудникам Департамента ИТ в соответствии с должностными обязанностями.

Пароль привилегированного пользователя может быть известен одновременно только одному, уполномоченному сотруднику Платежной организации.

Сетевые возможности рабочей станции, на которой осуществляется вход привилегированным пользователем, должны быть дополнительно ограничены специальными мерами, в частности на этой рабочей станции не разрешается использование ресурсов Интернет, управление службами или реестром по сети.

Действующие пароли привилегированных пользователей хранятся в закрытом виде в сейфе сотрудника, отвечающего за СУИБ Платежной организации.

Обеспечение антивирусной защиты

Информационная инфраструктура платежной организации связана с внешней средой (сетью Интернет), поэтому угроза проникновения вредоносного программного обеспечения весьма актуальна. Для защиты от этой угрозы применяются антивирусные средства. Правила внесения изменений в системы и информационную инфраструктуру в целом регламентированы во избежание проникновения вредоносного кода. В качестве антивирусного программного обеспечения может быть использовано только лицензионное ПО или ПО, распространяемое бесплатно.

Сервер

Сервер должен обязательно иметь установленное антивирусное программное обеспечение для автоматической проверки всех файлов и электронной почты, поступающих на этот сервер. Не реже 1 раза в неделю на терминальном сервере с установленной ОС должно проводиться полное сканирование всех дисков компьютера на предмет заражения вирусами. Антивирусное программное обеспечение на сервере должно обновляться не реже одного раза в день, автоматически путем соответствующих настроек антивирусного ПО.

Рабочие станции

Каждый персональный компьютер компании должен иметь установленное антивирусное программное обеспечение с функцией автоматической проверки всех файлов и электронной почты, поступающих на этот компьютер. Не реже 1 раза в неделю на каждом персональном компьютере Компании должно проводиться полное сканирование всех дисков компьютера на предмет заражения вирусами. Антивирусное программное обеспечение на персональных компьютерах должно обновляться не реже одного раза в день автоматически путем соответствующих настроек антивирусного ПО. При обнаружении заражения оперативной памяти компьютера любым вредоносным ПО, в процессе сканирования, зараженный компьютер должен быть немедленно отключен от локальной сети Платежной организации для дальнейшего тестирования и лечения.

Требования к программному обеспечению

Программное обеспечение, приобретаемое у сторонних лиц или разрабатываемое силами Платежной организации должно соответствовать требованиям информационной безопасности.

В целях разграничения доступа к информационным ресурсам в соответствии с принципом необходимости и достаточности в программном обеспечении должен быть обеспечен многоуровневый доступ к входным данным, функциям, операциям, отчетам, предусматривающим как минимум, четыре уровня:

Владелец;

Администратор;

Разработчик;

Пользователь.

Доступы предоставляются сотрудникам Платежной организации в соответствии с «Матрицей владельцев и администраторов информационных систем»

Программное обеспечение должно обладать защитой от ошибочных действий сотрудников, приводящих к событиям информационной безопасности. При выполнении функций или операций без полного заполнения всех обязательных полей программное обеспечение должно выдавать сообщение об ошибке.

Программное обеспечение должно обеспечивать оперативный и непротиворечивый поиск информации по критериям и параметрам, определенным для данного программного обеспечения, в том числе и за предыдущие даты, если такая информация подлежит хранению в программном обеспечении.

С целью мониторинга и журналирования действий сотрудников программное обеспечение должно обеспечивать сохранение запросов, обработку информации и ее хранение по дате и времени.

Отчеты, предоставляемые в Национальный Банк, а также отчеты о проведенных операциях должны формироваться автоматизировано, иметь возможность вывода выходных документов на экран, принтер или в файл.

В Платежной организации реализована возможность обмена электронными документами.

Обеспечение физической безопасности

Защита от несанкционированного физического доступа к компонентам информационной инфраструктуры является важнейшей задачей обеспечения информационной безопасности. Физический доступ сотрудников платежной организации и представителей внешних сторон к компонентам серверной информационной инфраструктуры ограничен и предоставляется только для выполнения должностных или договорных обязательств.

Мониторинг информационной инфраструктуры

Мониторинг информационной инфраструктуры необходим для своевременного выявления инцидентов и уязвимостей информационной безопасности. Мониторинг осуществляется в отношении производительности систем, доступа к данным, функционирования систем безопасности.

В информационных системах используется автоматизированное формирование журналов внутреннего учета средствами используемой операционной системы, дополнительно критичные события фиксируются в специализированном программном инструменте для мониторинга элементов ИТ-инфраструктуры:

локальная вычислительная сеть;

физические сервера;

виртуальные сервера;

прикладное программное обеспечение: сервисы обработки операций, системы управления базами данных;

При этом обеспечивается сбор и отображение основных метрик состояния, событий, а также формирование журнала\отчета событий за определенный диапазон дат или полностью.

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.

Для оценки общего уровня защищенности информационной инфраструктуры платежной организации выполняются проверки на уязвимости.

Независимый аудит системы безопасности и внутренних контролей проводится на регулярной основе не реже одного раза в год.

Обеспечение бесперебойной работы информационной инфраструктуры

Поскольку одной из задач СУИБ является обеспечение доступности информации, мерам по защите компонентов информационной инфраструктуры от сбоев отводится значительная роль.

Для обеспечения отказоустойчивости применяется дублирование критичных компонентов информационной инфраструктуры.

Средствами резервного копирования обеспечивается гарантированное восстановление бизнес-процессов после сбоя в работе одного или нескольких компонентов информационной инфраструктуры, а также обеспечивается минимизация времени восстановления сервисов и бизнес-процессов.

Резервированное копирование и восстановления данных, хранящихся в учетных системах, обеспечивается средствами используемых СУБД и Гипервизора VMware. 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.

Расположение оборудования, используемого для обработки и хранения баз данных в центрах обработки данных, отвечает требованиям:

гарантированное электропитание;

обеспечение необходимого климатического режима;

круглосуточный мониторинг и техническое обслуживание;

автоматический комплекс газового пожаротушения;

круглосуточно охраняемая территория;

системы видеонаблюдения;

разграничение физического доступа и организационные процедуры контроля доступа во все помещения;

порт выхода в сеть Интернет на скорости от 100 Мбит в секунду.

Платежная организация обеспечивает бесперебойное функционирование Системы в режиме 24/7/365 (24 часа в день, 7 дней в неделю, 365 дней в году), за исключением времени проведения профилактических работ.

Обучение и повышение осведомленности персонала в области информационной безопасности

Для достижения целей СУИБ с сотрудниками Платежной организации проводится работа по обеспечению готовности и способности к адекватным действиям в условиях угроз информационной безопасности.

Компетентность сотрудников Платежной организации обеспечивается с помощью процессов обучения, информирования персонала, а также периодической проверкой его компетентности в области информационной безопасности.

Все сотрудники Платежной организации несут персональную ответственность за нарушение установленных требований информационной безопасности.

Руководство Платежной организации несет ответственность за обеспечение информационной безопасности.

Организация и ответственность

Руководство платежной организации регулирует вопросы, связанные с:

- определением целей и стратегии достижения целей обеспечения информационной безопасности в платежной организации;
- выделением ресурсов для осуществления деятельности по обеспечению информационной безопасности в платежной организации;
- принятием решений в отношении ключевых рисков нарушения информационной безопасности.

Менеджер Департамента ИТ, или иное лицо, уполномоченное руководителем Платежной организации, несёт ответственность за:

- определение требований по информационной безопасности и осуществление контроля исполнения данных требований в платежной организации;
- осуществление контроля общей эффективности обеспечения информационной безопасности, её соответствия текущим и будущим требованиям бизнеса.

Владельцы процессов и активов несут ответственность за:

- распределение полномочий и ответственности по реализации мер обеспечения информационной безопасности (конфиденциальности, целостности, доступности) для своих активов, адекватных существующим рискам;
- устранение в установленные сроки несоответствий по результатам проведенных аудитов/проверок обеспечения ИБ.

Все работники платежной организации несут ответственность за соблюдение требований внутренних нормативных документов платежной организации, регламентирующих обеспечение информационной безопасности, а также своевременное оповещение о нарушениях и недостатках информационной безопасности, которые ими были обнаружены.

Ответственность работников Платежной организации за нарушение требований информационной безопасности определяется правилами внутреннего трудового распорядка платежной организации, а также положениями внутренних нормативных документов. В отдельных случаях, нарушение работниками требований информационной безопасности влечёт уголовную, административную, гражданско-правовую и иную ответственность, предусмотренную законодательством.

ГЛАВА 10. ОПИСАНИЕ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ И ОБОРУДОВАНИЯ, НЕОБХОДИМОГО ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖНЫХ УСЛУГ

10.1. Техническое описание сервиса и используемые технологии:

Платежная организация работает на платформе, установленной на серверах внутри Республики Казахстан;

АПК Платежной организации использует версию фреймворка Symfony 5.2, работает на php8;

Управление инфраструктурой осуществляется согласно принципам Infrastructure as Code, для управления виртуальными машинами в РК используется hashicorp terraform, для управления сервисами внутри виртуальных машин – ansible;

Защита от ddos осуществляется через Qrator;

Инфраструктура полностью соответствует требованиям стандарта PCI DSS, что подтверждается ежегодной успешной сертификацией аудитором Compliance Control.

10.2. Составляющие сервиса

Система представляет собой платформу для реализации платежей, обеспечения безопасности платежей, сбора и предоставления информации. Можно выделить отдельные логические блоки внутри сервиса:

Администратор;

Личный кабинет;

Интерфейс пользователя (UI);

Авторизация;

API;

Платежная форма;

Финансовая маршрутизация (провод денег через банки);

Антифрод;

Исторические данные;

Логи.

10.2.1 Администратор

Сервис реализует управление платформой администраторами платформы и службой технической поддержки из графического интерфейса. Он предоставляет возможность:

Подключить / отключить пользователя;

Задать / изменить настройки пользователя (набор сервисов, например, с каких платежных систем принимает деньги, нужны ли сервисы гаранта, бронирования товара, рассрочки, кредитования, рекомендаций и т. д.);

Просмотреть данные клиента: реквизиты (ИИН, адрес, расчетный счет и т. д.), договор, паспортные данные руководителя, соответствие параметров площадки клиента требованиям платформы (настоящие, а не тестовые товары на сайте, настоящие, а не тестовые материалы на сайте, контакты и реквизиты на сайте и т.д.), результат проверки клиента службой безопасности, способ ведения документооборота (бумажный / ЭДО), отметка о выпуске API ключа для проведения реальных платежей, в каких банках эквайерах клиент зарегистрирован, какие дополнительные платежные методы у клиента авторизованы, перечень запрошенных документов для расширения платежных методов (то, что запросили партнеры для авторизации);

- Просмотреть / изменить тариф клиента;
- Просмотреть активность и статистику клиента;
- Просмотреть / изменить настройки шлюза клиента;
- Просмотреть / изменить размещение контейнеров платформы по серверам;
- Просмотреть / изменить выделение ресурсов контейнерам платформы;
- Просмотреть логи и историю ошибок;
- Просмотреть / изменить настройки API-интеграций с партнерскими информационными системами (ИС);

- Просмотреть / изменить параметры маршрутизации;
- Просмотреть / изменить параметры антифрод системы.

10.2.2 Личный кабинет

Сервис обеспечивает управление подключением и личными настройками клиента:

- Регистрация на платформе;
- Предоставление материалов (документов) для регистрации и активации платежного сервиса;
- Управление настройками: перечень подключенных сервисов;
- Реквизит: (ИИН, адрес, расчетный счет и т. д.);
- Перечень предоставленных документов: договор, паспортные данные руководителя, выписки и справки;
- Соответствие собственного ресурса требованиям платформы и регуляторов;
- API ключ для проведения реальных платежей;
- Перечень запрошенных документов для расширения платежных методов;
- Тариф;
- История активности и статистика по платежам;
- Настройки шлюза;
- Выбор виджета для подключения к своему сайту. Платформа содержит ряд готовых модулей для самых популярных CMS. Клиент может выбрать наиболее подходящую форму для себя.

10.2.3 Авторизация

Этот сервис реализует полный протокол авторизации владельца карты или кошелька с эмитентом:

- Запрос авторизации сессии;
- Обмен авторотационными данными;
- Подтверждение авторизации.

10.2.4 API

Сервис содержит набор интерфейсов взаимодействия для всех ИС, с которыми установлены партнерские отношения, выполняет следующий функционал:

- Проверка к какому сервису будет проходить обращение;
- Проверка наличия всех необходимых данных для работы с выбранным сервисом;
- Сбор необходимых данных через форму взаимодействия с покупателем;
- Формирование запроса к выбранному сервису;
- Проведение выбранных операций: транзакций, запроса кредита, проверка платежеспособности и т.д;
- Возврат результат выполнения операции.

10.2.5 Платежная форма

Сервис предоставляет ряд платежных форм для разных клиентских CMS. Формы можно разделить на два отдельных кластера:

- Платежная форма (при оплате плательщик переходит на сайт агрегатора и там производит оплату);
- Платежный виджет (форма встраивается в сайт продавца, посредством iframe, плательщик не переходит на сайт агрегатора, но все данные вводятся и хранятся только на стороне агрегатора).

10.2.6 Финансовая маршрутизация (провод денег через банки)

Сервис обеспечивает маршрутизацию платежей. Так как платформа работает с большим пулом банков и имеет большое количество ежеминутных платежей, то это позволяет платформе собирать статистику о времени прохождения транзакций по разным маршрутам. При совершении транзакции платформа оценивает следующие параметры:

- Текущие маршруты проведения платежа;
- Скорость прохождения платежа по каждому из доступных маршрутов;
- Текущие очереди по каждому из маршрутов;
- Стоимость каждого маршрута. На основании этих данных формируется маршрут с учетом времени прохождения платежа и его стоимости (комиссий всех участников цепочки).

Сервис выполняет следующие проверки:

- Проверка карты / кошелька;
- Проверка наличия денежных средств на карте / кошельке;
- Проверка возможности совершения платежа. Сервис выполняет следующие действия:

- Подтверждает платеж;
- Регистрирует платеж;
- Формирует чек;
- Регистрирует платеж в платежной системе;
- Обновляет статус платежа.

10.2.7 Антифрод

Сервис антифрода базируется на собранной статистике за 7 лет проведения транзакций. На основе этой статистики сформированы следующие паттерны:

- Мошеннических платежей - эти платежи должны быть запрещены;
- Подозрительный платежей - эти платежи должны быть подтверждены дополнительными способами;
- Доверенных платежей - эти платежи можно пропускать быстро, с минимальной проверкой.

10.2.8 Исторические данные

Сервис собирает и хранит данные платежные данные по покупателям. Это позволяет покупателю в следующий раз провести оплату, не вводя весь набор платежных данных.

На основании этих данных накапливается информация об интересах покупателя:

- Торговые категории;
- Суммы покупок;
- Минимальные суммы по категориям;
- Максимальные суммы по категориям;
- Средние чеки по категориям;
- Частота покупок по категориям;
- Распределение покупок по времени (год, квартал, месяц, сутки).

10.2.9 Логи

Сервис собирает логи обо всех действиях системы. Это позволяет:

- Оперативно выявлять и устранять отказы;
- Выявлять причины отказа;

- Повышать отказоустойчивость системы;
- Прогнозировать причины отказа;
- Моделировать состояние системы при ее масштабировании и развитии.

ГЛАВА 11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Изменения и дополнения в Правила могут быть внесены по решению Директора ТОО «Open Trade» и подлежат обязательному направлению в уполномоченный орган в порядке и сроки, предусмотренные нормативными правовыми актами уполномоченного органа.

В случае если в результате внесения изменений и дополнений в законодательство Республики Казахстан, включая нормативные правовые акты уполномоченного органа, какие-либо положения настоящих Правил вступают в противоречие с новыми нормами законодательства, то до момента внесения изменений и дополнений в настоящие Правила действуют соответствующие нормы законодательства Республики Казахстан.