Утверждены
Решением единственного
участника №2
от «15» Сентября 2021 года

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ «Infinity Space»

Алматы 2021г.

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

Товарищество при наличии регистрационного номера учетной регистрации платежной организации, присвоенного Национальным Банком Республики Казахстан, оказывает 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.

1. Термины и определения

В Правилах используются понятия, предусмотренные законами Республики Казахстан «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», а также следующие понятия:

- ✓ **Клиент** - физическое или юридическое лицо, филиал или представительство юридического лица, индивидуальный предприниматель получающие платежную услугу.
- ✓ **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, применяемые новые технологий, внедрение новых продуктов и т.д.).
- ✓ **Мерчант** – Клиент, юридическое лицо, в том числе банк второго уровня или индивидуальный предприниматель, являющийся Участником расчетов и осуществляющее(-ий) коммерческую деятельность и принимающее(-ий) оплату от Клиентов-физических лиц в качестве оплаты по гражданско-правовым сделкам на основе договора.
- ✓ **НСД** - несанкционированный доступ к Системе.
- ✓ **Авторизация** – процедура запроса и последующего получения Мерчантом от ТОО «Infinity Space» согласия на проведение Операции оплаты с использованием Платежной карточки в Интернет-магазине. Указанное согласие содержит уникальный код (код Авторизации), идентифицирующий каждую конкретную Операцию оплаты.
- ✓ **Одностадийная Авторизация** – Операция оплаты, при которой вся сумма платежа сразу списывается с платежной карточки Покупателя.
- ✓ **Двустадийная Авторизация** – Операция оплаты, при которой сумма платежа на первой стадии резервируется (холдируется) на счете, к которому выпущена платежная

карточка Покупателя, а на второй стадии, после подтверждения Авторизации Мерчантом, списывается с платежной карточки Покупателя.

- ✓ **АПК** – специализированный аппаратно-программный комплекс ТОО «Infinity Space» и (или) Банка.
- ✓ **Банк** – 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.
- ✓ **Банк-эмитент** – банки, осуществляющие выпуск платежных карточек, в том числе Банк.
- ✓ **Банк-эквайер** – Банк, обеспечивающий проведение Операций по платежным карточкам.
- ✓ **Возвратный платеж** – требование эмитента в отношении транзакции, составленное в соответствии с Правилами Международных платежных систем, включая первое и все дальнейшие требования в отношении одной Транзакции.
- ✓ **Данные транзакции** – информация о Транзакции и Карте, с помощью которых была проведена Транзакция, а также информация о результатах идентификации Держателя карты.
- ✓ **Держатель платежной карточки (Покупатель)** – законный держатель Карты, использующий Карту для совершения Операций.
- ✓ **Интернет-магазин** – электронная среда, в которой Интернет-компания осуществляет коммерческую деятельность посредством реализации своих товаров и услуг.
- ✓ **Итоговый реестр платежей** – отчет в электронном виде, формируемый Платежной организацией 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 Платежной организацией самостоятельно.
- ✓ **Личный кабинет (ЛК)** – личный кабинет Мерчанта, посредством которого Мерчант имеет возможность самостоятельно просматривать информацию об Операциях, инициировать проведение Операций возврата/отмены оплаты.
- ✓ **Мошенническая транзакция** – транзакция, проведенная с использованием поддельной, украденной или утерянной карты, умышленно искаженных данных карты, либо транзакция, проведенная другим незаконным способом.
- ✓ **Международные платежные системы** (МПС) – международные платежные системы: Visa International и MasterCard International и иные МПС.
- ✓ **Обработка Операций (Процессинг)** – обработка ТОО «Infinity Space» 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.
- ✓ **Операция (Операции)** – общее определение, включающее в себя следующие виды операций: Операцию оплаты, Операцию отмены оплаты, Операцию возврата, Операцию отмены возврата.
- ✓ **Операция оплаты** – оплата Покупателем услуг Мерчанта в Интернет-магазине с использованием платежной карточки.

- ✓ **Операция отмены оплаты** – инициированная одной из Сторон отмена ранее произведенной Операции оплаты в связи с ошибкой или техническим сбоем при ее проведении.
- ✓ **Операция возврата** – операция по возврату денег Покупателю по проведённой Покупателем Операции оплаты, в связи с его отказом от Услуги (возвратом товара) Мерчанта, инициированная Мерчантом. Операция возврата осуществляется исключительно с использованием платежной карточки, по которой Покупателем ранее была совершена Операция оплаты. Выдача наличных денег в случае возврата товара, ранее оплаченного с использованием платежной карточки, запрещается.
- ✓ **Операция отмены возврата** – отмена ранее произведенной Операции возврата, инициированная Мерчантом.
- ✓ **Платежная карточка (Карта)** – банковская карточка МПС.
- ✓ **Специальный (транзитный) счет** – счет Банка, предназначенный для учета зачисления денег по распоряжениям Клиентов, и учета дальнейшего их перевода в пользу Мерчантов, а также проведения иных взаиморасчетов между Платежной организацией и Клиентами при оказании платежных услуг.
- ✓ **Способ платежа** – канал/способ осуществления Операции оплаты в Интернет-магазине с использованием Карты в качестве электронного средства платежа.
- ✓ **Транзакция** – финансовая операция с картой, в результате которой производится оплата каких-либо товаров или услуг, или перевод на карту.
- ✓ **Шлюз** – программное обеспечение для создания электронного канала посредством которого производится обмен Данными по транзакциям и данными.
- ✓ **Система** – совокупность программно-технических средств, документации и организационно-технических мероприятий, обеспечивающих информационно-технологическое взаимодействие, регистрацию и осуществление платежей и иных операций в соответствии с настоящими Правилами осуществления деятельности платежной организации ТОО «Infinity Space».
- ✓ **Процессинг -** обработка ТОО «Infinity Space» 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.

СОДЕРЖАНИЕ ПРАВИЛ:

1. Описание платежных услуг, оказываемых платежной организацией

Согласно учетной регистрации платежной организации, проведенной Национальным Банком Республики Казахстан, ТОО «Infinity Space» оказывает 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.

2. Порядок и сроки оказания платежных услуг клиентам Платежной организации.

2.1. 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.

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

В рамках исполнения/оказания данной услуги Платежная организация в соответствии с договором, заключенным с Банком, обеспечивает прием платежей инициированных Клиентом 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.

Инициация клиентом операций/ платежей производится посредствам WEB – приложений, online -приложений, мобильных приложений (приложений для мобильных устройств), программного обеспечения, терминалов самообслуживания, виджетов и прочих приложений - обеспечивающих возможность инициации клиентом в электронной форме распоряжений на списание денег с платежной карты Клиента с целью последующего исполнения поручения/ распоряжения Клиента полученного Платежной организацией от Клиента и переданного Платежной организацией в Банк.

2.1.2. При оказании услуги Платежная организация обеспечивает следующий алгоритм действий:

- ✓ Клиент взаимодействует с Платежной организацией, осуществляя выбор необходимой ему услуги из перечня услуг, предоставляемых Интернет-магазином, с учетом Способа Платежа.
- ✓ Для осуществления оплаты проводится Авторизация в зависимости от выбранного Клиентом Способа Платежа, при этом Авторизация может быть Одностадийной и Двустадийной:

1) Одностадийная Авторизация – Операция оплаты, при которой вся сумма платежа сразу списывается с платежной карты Клиента.
2) Двустадийная Авторизация – Операция оплаты, при которой сумма платежа на первой стадии резервируется (холдируется) на счете, к которому привязана платежная карта Клиента, а на второй стадии, после подтверждения Авторизации Мерчантом, списывается с указанной карты Клиента.

- ✓ Мерчант по согласованию с Платежной организации выбирает наиболее удобный для себя вариант, если иное не устанавливается Платежной организацией для данного конкретного Мерчанта. В случае проведения Двустадийной Авторизации операции Мерчант должен осуществить завершение второй стадии в течение 15 календарных дней со дня проведения первой стадии Авторизации.
- ✓ Перевод Банком денег Мерчанту осуществляется после обработки операций в срок, не позднее 3 (трех) рабочих дней от даты обработки Авторизации операций. При этом Процессинг Двустадийной Авторизации проходит только после успешного завершения обеих стадий.

Порядок проведения Авторизации:

- ✓ Клиент в специальной электронной форме с использованием имеющегося у него компьютера/мобильного телефона/иного электронного устройства вводит реквизиты Карты, используемой для Операции оплаты.
- ✓ По запросу Платежной организации Клиент вводит дополнительные данные в зависимости от используемой технологии повышения безопасности платежей, в соответствии с правилами МПС.
- ✓ Платежная организация осуществляет Авторизацию с предоставленными Клиентом реквизитами – в соответствии с Правилами МПС.
- ✓ Платежная организация информирует Мерчанта о результате Авторизации – согласии с проведением Операции или отказе в проведении Операции.

2.1.3. В случае возврата/отказа Клиентом от Услуги, либо необходимости проведения отмены ранее осуществленной Операции оплаты, Мерчант инициирует проведение таких операций в ЛК.

2.1.4. 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.

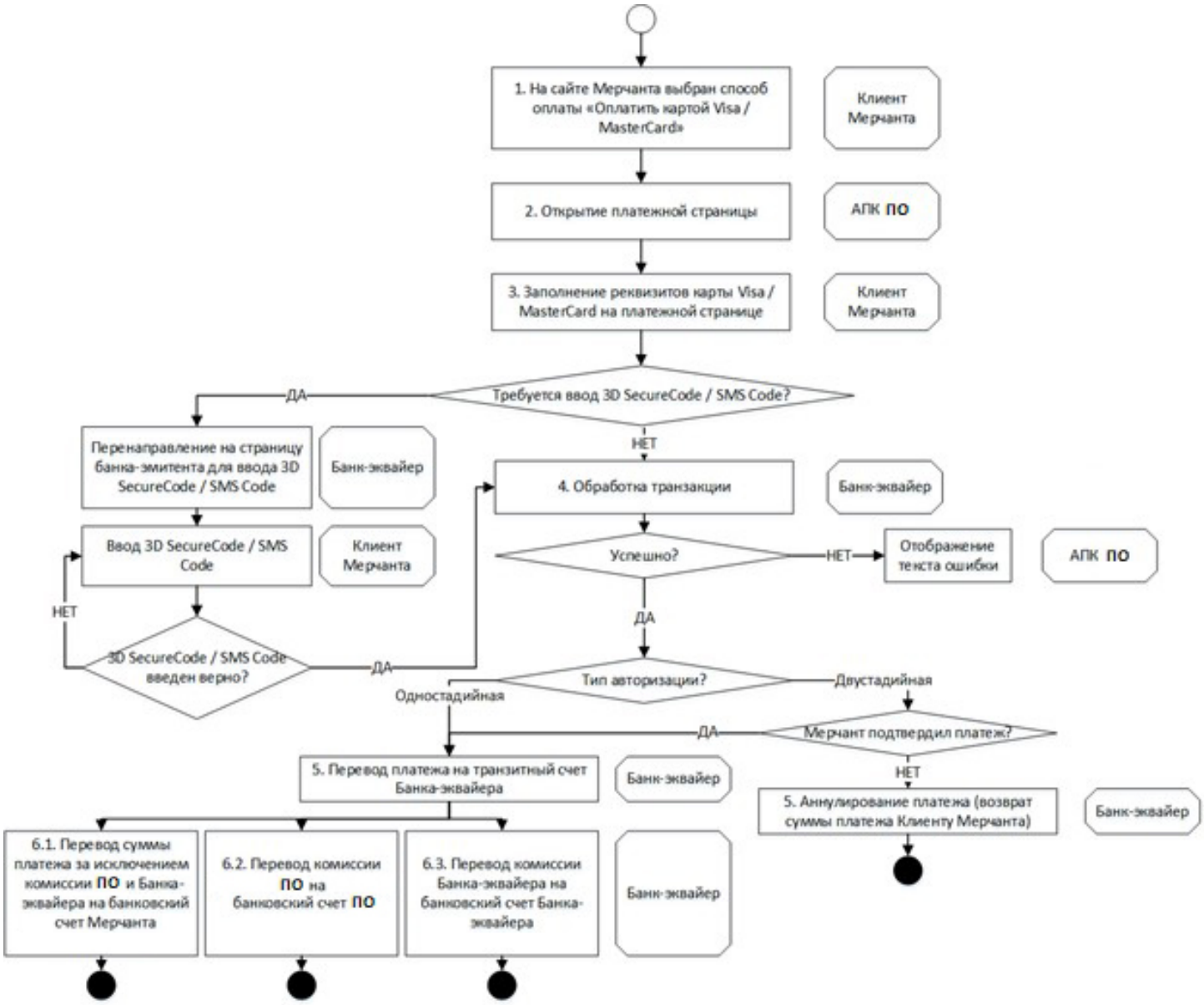
2.1.5. Платежная организация на периодической основе - один раз в сутки, и в соответствии с Правилами МПС осуществляет Обработку Операций, совершенных с момента предыдущего цикла обработки Операций. При этом в случае, если для совершения Авторизации был использован Способ Платежа – Двустадийная Авторизация, Платежная организация осуществляет Обработку Операций в отношении таких Авторизаций только после получения Платежной организацией от Мерчанта запроса (так называемое «завершение авторизации»), подтверждающего необходимость Обработки Операции.

2.1.6. По результатам Обработки Операций Платежная организация направляет Мерчанту Отчет по успешно прошедшим транзакциям.

2.1.7. Порядок проведения расчетов:

- ✓ На сайте Мерчанта выбран способ: оплатить картой
- ✓ Открытие платежной страницы
- ✓ Заполнение реквизитов платежной карты
- ✓ Обработка операции
- ✓ получение статуса операции, в случае получения статуса: успешно, осуществляется перевод платежа на счет банка-эквайера, используемый банком-эквайером для расчетов с Мерчантом;
- ✓ Перевод денег со счета банка-эквайера на счет Мерчанта, за исключением вознаграждения Платежной организации и комиссии Банка-эквайера или перевод денег 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.



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

- ✓ Банк-эмитент осуществляет списание денег с карты Клиента;
- ✓ Банк – эмитет осуществляет платеж в пользу Банка-эквайера;
- ✓ Банк-эквайер перечисляет платеж на счет Мерчанта.

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

2.1.9. 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 платежных системах.

2.1.10. Завершение операционного дня

По итогам операционного дня Платежная организация направляет реестр платежей банку-эмитенту для завершения расчетов с Мерчантами (перевод денег на банковский счет Мерчанта со счета банка-эквайера) и распределения комиссии между самим банком-эквайером и Платежной организацией.

После завершения расчетов по операциям, проведенным в течение операционного дня Платежная организация направляет отчетный реестр Мерчанту по платежам, проведенным в пользу него.

Срок оказания услуги: в течение 1 операционного дня.

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

3.1 Виды, размер, порядок взимания комиссий определяется сторонами Договора при оказании Платежной организацией услуг исходя из действующих рыночных тарифов на услуги подобного вида, с учетом сумм комиссий, подлежащих в последующем перечислению третьим лицам (Мерчантам, лицам, обеспечивающим технологическое взаимодействие с Платежной организацией при оказании последними платежных услуг).

3.2 Перечень тарифов, также, как и размер комиссий/тарифов не является фиксированным и может быть изменен, дополнен или отменен Платежной организацией в одностороннем порядке с обязательным согласованием с контрагентами (Мерчантам с обязательным уведомлением Клиентов в соответствии с настоящими Правилами **и положениями Публичного договора**, размещенного на Сайте Системы.

3.3 Платежная организация оставляет за собой право взимать специальные комиссии за дополнительные виды услуг (работ) или за нестандартные операции, исполняемые по поручению Клиента и не предусмотренные установленным перечнем.

3.4 Суммы комиссий, указанные в настоящих Правилах, могут также включать в себя комиссии, взимаемые партнерами Платежной организации, в пользу которых осуществляются платежи.

3.5 Стоимость услуг определяется в зависимости от тарифов банка-эсквайра и составляет 0% до 5% с каждой транзакции.

3.6 Платежная организация в вправе предоставлять отдельным Мерчантам индивидуальные скидки к утвержденным тарифам, а таже условия варьируются, в зависимости от категории Мерчанта.

Платежная организация имеет право устанавливать минимальную комиссию (вознаграждение), вне зависимости от процентной ставки.

4. Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией.

Технологическое обеспечение платежных услуг оказывается Платежной организацией самостоятельно путем обеспечения информационного и технологического взаимодействия между участниками расчетов, включающего сбор, обработку и рассылку информации, между участниками расчетов, путем предоставления доступа к программному обеспечению Платежной организации клиентам.

Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых Платежной организацией происходит на основании договоров, заключенных с третьими лицами.

Взаимодействие Платежной организации с третьими лицами при оказании платежных услуг подлежит осуществлению в строгом соответствии с требованиями законодательства Республики Казахстан.

При взаимодействии с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых Платежной организацией, принимаются надлежащие меры безопасности, в том числе позволяющие обеспечить зависящую от соответствующей стороны взаимодействия информационную безопасность, защищенность персональных данных и иной информации, подлежащей обязательной защите в соответствии с законодательством Республики Казахстан.

Подключение информационных систем третьей стороны к системам Платежной организации производится только на основании заключённого договора и соглашения о неразглашении конфиденциальной информации.

Техническое взаимодействие с платёжными сервисами третьей стороны может осуществляться:

- в отладочном режиме в период технической интеграции;
- в режиме эксплуатации.

В соответствии с требованиями бизнеса и рисков, связанных с утечкой и разглашением конфиденциальной информации, к которой осуществляется доступ третьей стороной, работниками отдела информационных технологий по согласованию с третьей стороной осуществляется контроль должного уровня обслуживания и уровня информационной безопасности третьей стороны.

Контроль может включать:

- анализ отчётов о работах (услугах), предоставляемых третьей стороной;
- регулярные совещания по вопросам и проблемам, возникающим в ходе работ;
- анализ отчётов и результатов расследования возникших инцидентов информационной безопасности.

Порядок взаимодействия Платежной организации с соответствующим банком, осуществляющим перевод денег по оказываемым платежным услугам.

Порядок взаимодействия Платежной организации с Банком, осуществляющим перевод денег по оказываемым платежным услугам, определяется на основании договора. Вся информация о принятых платежах/обработанных операциях отражается в реестре платежей в электронной форме, в режиме реального времени. Указанный реестр сверяется с реестрами Мерчантов. После сверки реестров Платежная организация формирует реестр платежей/операций за отчетный период и передает его получателю реестра, в соответствии с условиями договоров.

5. Сведения о системе управления рисками, используемой платежной организацией

В основные задачи системы управления рисками, используемой Платежной организацией 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.

В целях эффективного управления рисками платежная организация 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.

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

1) размер, характер и сложность бизнеса;

2) доступность рыночных данных для использования в качестве исходной информации;

3) состояние информационных систем и их возможности;

4) квалификацию и опыт персонала, вовлеченного в процесс управления рыночным риском.

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

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

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

своевременно и последовательно использовать все возможности развития платежной организации и одновременно удерживать риски на приемлемом и управляемом уровне.

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

В основу управления рисками положены следующие принципы:

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

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

Мероприятия по управлению рисками:

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

2) определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих работников Платежной организации;

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

4) определение показателей бесперебойности функционирования Платежной организации;

5) определение порядка обеспечения бесперебойности функционирования платежной организации;

6) определение методик анализа рисков;

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

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

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

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

11) определение порядка обеспечения защиты информации в Платежной организации.

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

Способы управления рисками:

1) управление очередностью исполнения распоряжений должностными лицами;

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

3) обеспечение возможности предоставления лимита;

4) использование безотзывных банковских гарантий;

5) отказ от взаимодействия с неблагонадежными партнерами;

6) страхование возможных рисков;
7) другие способы управления рисками.

6. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами

В целях контроля за качеством оказываемых услуг Платежной организацией предпринимается комплекс мер, направленных на предупреждение и урегулирование спорных ситуаций при оказании услуг клиентам. Платежной организацией проводится обучение персонала, который сможет своевременно урегулировать любую спорную ситуацию.

Платежная организация ведет контроль качества оказываемых услуг и принимает своевременные меры по предупреждению и устранению нарушений оказания услуг клиентам. Все спорные ситуации разрешаются путем переговоров с клиентами. В случае не достижения сторонами спора положительного результата, спор подлежит разрешению в претензионном порядке на основании письменной претензии клиента в течение 15 календарных дней с момента получения платежной организацией такой претензии/заявления.

Платежная организация вправе запросить у клиента оригинал чека или иных документов, подтверждающих проведение платежа. В случае если услуга осуществлялась в безналичной форме платежная организация производит сверку всех операций, произведенных с участием клиента с банком и другими участниками расчетов.

Если возникший спор не будет урегулирован в претензионном порядке в течение 15 календарных дней, он подлежит рассмотрению в судебном порядке в соответствии с законодательством Республики Казахстан.

Все претензии, касающиеся вопросов качества товаров/услуг Получателя Перевода, а также реализации и защиты прав потребителей, в части обмена и возврата товара/услуг направляются Клиентом непосредственно в адрес получателя Перевода.

7. Порядок соблюдения мер информационной безопасности

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

Методами обеспечения защиты информации в Платежной организации являются:

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

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

Идентификация пользователей, персонала и ресурсов информационной системы.

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

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

Регистрация (протоколирование) обращений к защищаемым объектам и информации.

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

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

1. Защита информационной системы Платежной организации осуществляется с целью исключения возможностей:

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

2. Защита системы от несанкционированного доступа.

2.1. Права администратора программно-аппаратных средств защиты от несанкционированного доступа к системе (далее – НСД) предоставляются уполномоченному сотруднику оператора, ответственному за обеспечение безопасности организации.

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

- ✓ Наличие пароля для ограничения доступа к личному кабинету пользователя, обеспечивающего защиту информации от несанкционированной модификации или уничтожения.
- ✓ обеспечение безопасных условий эксплуатации аппаратно-программных средств и исключение несанкционированного доступа к ним.
- ✓ координацию деятельности участников системы по обеспечению защиты от НСД;
- ✓ постоянный мониторинг оператором уровня защиты от НСД;
- ✓ выявление факторов риска нарушения защиты от НСД, определения степени и характера влияния факторов риска на защиту от НСД;
- ✓ проведение расследований событий, вызвавших операционные сбои, анализ их причин и последствий;
- ✓ принятие мер по устранению или минимизации рисков защиты от НСД.
- ✓ контроль соблюдения требований правил, договорных обязательств Участниками в части обеспечения бесперебойности работы и обеспечения безопасности Системы;
- ✓ обеспечения сохранения функциональных возможностей операционных и технических средств, информационных систем при сбоях;

- ✓ проведение тестирования для выявления недостатков, принятие мер по устранению выявленных недостатков.

2.3. Уровень риска нарушения защиты НСД определяется в зависимости от степени угрозы и вероятности возникновения риска:

I (низкий) – уровень риска, в результате которого возможные/выявленные нарушения не оказывают влияние на защиту от НСД;

II (средний) – уровень риска, в результате которого возможные/выявленные нарушения оказывают влияние на защиту от НСД в незначительной мере;

III (допустимый) – уровень риска, в результате которого возможные/выявленные нарушения оказывают влияние на защиту от НСД в допустимой мере;

IV (высокий) – уровень риска, в результате которого возможные/выявленные нарушения оказывают влияние на защиту от НСД в значительной мере;

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

3. Требования по организации хранения и использования паролей:

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

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

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

3.4. Длина паролей должна составлять не менее шести символов.

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

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

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

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

3.9. В случае подозрения на компрометацию пароля доступа к личному кабинету необходимо незамедлительно произвести его замену. В случае отсутствия возможности немедленной замены пароля, необходимо связаться с эмитентом или оператором для блокировки электронного кошелька.

3.10. Запрещается:

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

4. Рекомендации по защите от различных видов мошенничества.

4.1. SMS мошенничество. SMS используется мошенниками для сбора информации под различными предлогами. Данные сообщения часто похожи на настоящие официальные сообщения от банка. Однако следующие признаки помогут Вам отличить сообщения, присланные мошенниками:

- ✓ Запрашиваемые в них действия требуют срочного ответа. Например, счет будет закрыт или временно заблокирован.
- ✓ Требуют предоставить, обновить или подтвердить персональные данные (кодовое слово, пароль и т.д.)
- ✓ Содержат форму для ввода персональных данных.

- ✓ Содержат информацию, что на кошелек поступили деньги, которых пользователь не ожидал.
- ✓ Просят пройти по ссылке в сообщении.
- ✓ Просят подтвердить что-либо, ответив на SMS. В этом случае, скорее всего, с мобильного телефона могут быть списаны значительные средства.

4.2. Мошенничество по электронной почте.

Фишинг (phishing) — это искаженное слово от английского слова fishing (ловить рыбу). Этим термином называют наиболее распространенную форму мошенничества в сети Интернет. Злоумышленники используют сообщение электронной почты, отправленное огромному количеству пользователей Интернет, и надеются, что кто-нибудь «попадется» в расставленные сети размером с Интернет и отправит им свои данные. Сообщения электронной почты, которые используются в качестве приманки, часто похожи на настоящие официальные сообщения. Однако, их целью является заманить клиента на фальшивые веб-сайты, замаскированные под сайты известных организаций, например, банков, чтобы получить пользовательские персональные данные (номер банковской карты, пароль, ПИН код) и использовать данную информацию для кражи средств с вашего банковского счета. Даже если пользователь просто переходит по ссылке на фальшивый сайт и не согласились передать им персональные данные, компьютер может быть заражен вирусом, который будет сканировать нажатие клавиш клавиатуры и передавать злоумышленникам пользовательские персональные данные, вводимые на подлинном сайте. Если же пользователь вводит, например, свой номер телефона, то на телефон может быть отправлено (в зависимости от модели телефона) сообщение с вирусом, позволяющее злоумышленнику перехватывать все сообщения.

Наиболее характерные признаки того, что письмо прислано мошенниками:

- ✓ Запрашиваемые в них действия требуют срочного ответа. Например, пользовательский счет будет закрыт или временно заблокирован.
- ✓ Сообщения содержат ссылки на страницы Интернет, которые похожи на настоящие (они могут содержать название банка или написаны похожим образом). Однако все эти ссылки ведут на фальшивый сайт или открывают всплывающее окно, которое запрашивает или требует подтвердить персональные данные.
- ✓ Такие сообщения могут содержать явные опечатки или орфографические ошибки, что позволяет им обходить «spam» фильтры, установленные у Интернет провайдеров.

Банк никогда:

- ✓ Не отправляет сообщения с просьбой подтвердить, обновить или предоставить персональные данные, имя пользователя и пароль, кодовое слово и т.п.
- ✓ Не просит зайти по ссылке в письме, т.к. это противоречит соображениям безопасности.

4.3. Телефонное мошенничество.

Звонки по телефону, наряду с сообщениями электронной почты и СМС, используются мошенниками для сбора конфиденциальной информации, часто похожи на «настоящие» звонки. Если пользователь получил подозрительный телефонный звонок от имени банка, необходимо уточнить цель звонка, отдел, далее связаться с банком, чтобы уточнить подлинность данного звонка. Также необходимо уточнять случаи получения подозрительных писем по почте (в т.ч. электронной) от имени банка.