Утверждены Решением единственного
Участника №05 от 2 августа 2024 г.
Введены в действие приказом
Директора № П-02-08-2024
от 2 августа 2024 г.
А. Еркеевой

Правила осуществления деятельности платежной организации ТОО «Irbis Tech»

Редакция 5.0
г. Алматы, 2024г.

ОГЛАВЛЕНИЕ

Настоящие Правила осуществления деятельности платежной организации ТОО «Irbis Tech» (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, Уставом ТОО «Irbis Tech» и определяют порядок организации деятельности ТОО «Irbis Tech» (далее как указано ранее или Irbis Tech или ТОО, или Платежная организация, или Организация) в качестве платежной организации.

Товарищество при наличии регистрационного номера учетной регистрации платежной организации, присвоенного Национальным Банком Республики Казахстан, оказывает следующие виды платежных услуг:

1) 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

1) **Авторизация** – процедура запроса и последующего получения Мерчантом от ТОО «Irbis Tech» согласия на проведение Операции оплаты с использованием Платежной карточки в Интернет-магазине. Указанное согласие содержит уникальный код (код Авторизации), идентифицирующий каждую конкретную Операцию оплаты.
2) **Одностадийная Авторизация** – Операция оплаты, при которой вся сумма платежа сразу списывается с платежной карточки Покупателя.
3) **Двухстадийная 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.
4) **АПК** – специализированный аппаратно-программный комплекс ТОО «Irbis Tech», Банка.
5) **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.
6) **Банк-эмитент** – банки, осуществляющие выпуск платежных карточек, в том числе Банк.
7) **Банк-эквайер** – Банк, обеспечивающий проведение Операций по платежным карточкам.
8) **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.
9) **Данные транзакции** – информация о Транзакции и Карте, с помощью которых была проведена Транзакция, а также информация о результатах идентификации Держателя карты.
10) **Держатель платежной карточки (Покупатель)** – законный держатель Карты, использующий Карту для совершения Операций.
11) **Интернет-магазин** – электронная среда, в которой Мерчант осуществляет коммерческую деятельность посредством реализации своих товаров и услуг.
12) **Итоговый реестр платежей** – отчет в электронном виде, формируемый Irbis Tech 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 Irbis Tech самостоятельно.
13) **ЛК** – личный кабинет Мерчанта, посредством которого Мерчант имеет возможность самостоятельно просматривать информацию об Операциях, инициировать проведение Операций возврата/отмены оплаты.
14) **Мерчант** – юридическое лицо или физическое лицо, осуществляющее деятельность без образования юридического лица (индивидуальный предприниматель), в соответствии с регулирующим законодательством принимающий платежи в свою пользу от Держателей платежной карты, и реализующий товары, услуги последним посредством Интернет - магазина.
15) **Мошенническая транзакция** – транзакция, проведенная с использованием поддельной, украденной или утерянной карты, умышленно искаженных данных карты, либо транзакция, проведенная другим незаконным способом.
16) **Международные платежные системы (МПС)** – международные платежные системы: Visa International и MasterCard International.
17) **Обработка Операций (Процессинг)** – обработка ТОО «Irbis Tech» 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.

18) **Операция (Операции)** – общее определение, включающее в себя следующие виды операций: Операцию оплаты, Операцию отмены оплаты, Операцию возврата, Операцию отмены возврата.
19) **Операция оплаты** – оплата Покупателем услуг Мерчанта в Интернет-магазине с использованием платежной карточки.
20) **Операция отмены оплаты** – инициированная одной из Сторон отмена ранее произведенной Операции оплаты в связи с ошибкой или техническим сбоем при ее проведении.
21) **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.
22) **Операция отмены возврата** – отмена ранее произведенной Операции возврата, инициированная Мерчантом.
23) **Платежная карточка (Карта)** – банковская карточка МПС.
24) **Система ТОО «Irbis Tech» (сокр. Система)** - совокупность программно-технических средств, документации и организационно-технических мероприятий, обеспечивающих осуществление платежей и иных операций, как инициированных клиентом в электронной форме, так и с использованием электронных денег.
25) **Специальный счет** – внутренний учетный счет Расчетного банка, прикрепленный к Основному банковскому счету Организации (расчетный счет Организации), для учета зачисления денежных средств по Распоряжениям Держателей платежных карт, и учета дальнейшего их перевода в пользу Получателей, для учета дебиторской задолженности Компании перед последними, а также для учета выплаты вознаграждения Расчетному банку, и проведения иных взаиморасчетов между Компанией и Получателями в рамках Договора оказания услуг.
26) **Расчетный банк** – Банк и(или) Банк-эквайер в котором для Организации открыт Специальный счет.
27) **Способ платежа** – канал/способ осуществления Операции оплаты в Интернет-магазине с использованием Карты в качестве электронного средства платежа.
28) **Транзакция** – финансовая операция с картой, в результате которой производится оплата каких-либо товаров или услуг.
29) **Распоряжение** – указание - распоряжение инициатора платежа и (или) перевода денег Мерчанту об осуществлении платежа и (или) перевода денег, которое выражается в форме поручения, требования или в виде согласия Держателя платежной карты; электронный документ, содержащий поручение Держателя платежной карты на перевод денежных средств в пользу Мерчанта в счет оплаты Товаров (услуг), а также информацию, необходимую для его исполнения, составленный и переданный с посредством АПК Организации, Банку-эквайеру и (или) Банку в целях последующего осуществления Операции оплаты.
30) **Центр обмена данными по платежным транзакциям с признаками мошенничества (далее – антифрод-центр)** – юридическое лицо Национального Банка Республики Казахстан, которое осуществляет меры, направленные на предотвращение платежных транзакций с признаками мошенничества

2. Описание платежных услуг

2.1. Платежная организация 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 (далее «Услуги»):

1) Прием платежей по картам Visa, MasterCard и других МПС.

2.1.1. Схема приема платежей по картам Visa, MasterCard и других МПС

- Клиент Мерчанта со страницы его сайта переходит на страницу оплаты.
- Клиент Мерчанта вводит реквизиты карты (тип карты, имя держателя карты, номер карты, срок действия карты, CVV).
- Если Мерчант выбрал одностадийную схему проведения платежа, Irbis Tech передает Банку информацию о списании заявленной суммы с карты, после чего Банк, либо Банк – эквайер передает информацию Банку – эмитенту, Банк - эмитент списывает сумму с карты клиента Мерчанта и Банк зачисляет сумму на расчетный счет Мерчанта или Специальный счет, открытый для Платежной организации для расчетов с Мерчантами.
- Если Мерчант выбрал двухстадийной схему проведения платежа:
- Irbis Tech передает Банку информацию о блокировке указанной суммы и Банк/Банк –эквайер блокирует сумму на карте клиента Мерчанта.
- Если Мерчант подтверждает операцию, в этом случае Irbis Tech передает Банку информацию о списании указанной суммы с карты клиента мерчанта и Банк/Банк эквайер передает информацию Банку – эмитенту, Банк - эмитент списывает сумму с карты клиента Мерчанта.
- Если Мерчант не подтверждает операцию. Irbis Tech не передает информацию о списании суммы Банку и Банк- эмитент не списывает сумму с карты клиента Мерчанта.

3. Порядок и сроки оказания платежных услуг

3.1. Для получения Услуг Irbis Tech Мерчанту необходимо:

- иметь зарегистрированное юридическое лицо (либо статус индивидуального предпринимателя),
- работающий интернет-сайт
- счет в любом банке второго уровня РК.

3.2. Стандартные этапы подключения:

- Мерчант подает заявку на подключение (заявка подается на сайте Организации, или письменно, путем отправки заявки по e-mail)

Заявка на подключение должна содержать наименование и URL-адрес сайта Мерчанта, номер телефона и email представителя Мерчанта. При этом, сайт Мерчанта должен отвечать следующим требованиям:

- URL-адрес и все внутренние ссылки сайта Мерчанта должны быть рабочими и адекватно обрабатываемыми.
- Сайт Мерчанта не должен предоставлять услуги «развлечений для взрослых» («Adult Entertainment»).
- На электронной витрине сайта Мерчанта не должно быть ссылок или баннеров подозрительных сайтов (например, сайтов для взрослых и т.п.), а также ссылок баннерных сетей, в которых могут всплыть баннеры подозрительного содержания.
- Сайт не должен располагаться на бесплатных серверах, предоставляющих услуги хостинга.
- Наличие на сайте актуальной справочной информации о Мерчанте. Обязательным условием является наличие наименования страны, адреса места нахождения, адреса для корреспонденции (адрес не может быть до востребования), а также контактных телефонов, по которым клиент может связаться со службой поддержки сайта.
- Перечень продаваемых товаров (работ, услуг), перечисленных в анкете Мерчанта, должен соответствовать перечню товаров (работ, услуг), предлагаемых на сайте.
- Полнота описания потребительских характеристик продаваемых товаров (работ, услуг). (Проверяется для того, чтобы недостаток описания товара, работы, услуги не мог стать причиной для возврата платежа). В том числе, в обязательном порядке на сайте должны быть указаны цены на товары, работы, услуги.
- Реквизиты банковской карты не должны приниматься на сайте. Для оплаты с использованием карты клиент должен обязательно переадресовываться на АПК Организации.

- Наличие на сайте описания процедур заказа товаров (работ, услуг) и их оплаты с использованием карт. Также обязательным условием является наличие на сайте формы оплаты товара (работы, услуги) с использованием карт.
- Наличие на сайте информации по доставке товара (получении работы, услуги), такой как сроки, способы, а также любой другой информации, необходимой для получения ясного представления о доставке товара (получении работы, услуги) после оплаты с использованием карты.
- Наличие на сайте описания процедур возврата денег, предоставления взаимозаменяемых товаров, обмена товаров и т.п. при отказе от товара (работы, услуги). В случае если такие процедуры Мерчантом не предусмотрены, то он обязан информировать об этом на своем сайте.
- Мерчант обязан предусмотреть осуществление контроля получения заказов клиентами.
- Мерчант обязан предусмотреть методы ограничения и контроля рисков мошеннических операций. Обязательным условием является применение при этом возможностей АПК Irbis Tech по борьбе с мошенничеством.
- Все страницы, которые связаны с работой сайта, должны находиться под единым доменным именем.
- Наличие предупреждения о том, что посещение сайта, приобретение и доставка клиента конкретного товара (работы, услуги) могут быть незаконными на территории страны, где находится клиент.
- Наличие предупреждения о том, что клиент несет ответственность за невыполнение законов своей страны при посещении данного сайта и попытке приобрести товары (работы, услуги), если таковые запрещены законодательством на территории страны, где он находится.

3.3. Для заключения договора на оказание услуг Организации, Мерчант предоставляет следующие документы:

ДЛЯ ЮРИДИЧЕСКИХ ЛИЦ

- документ(-ы), удостоверяющий(-ие) личность должностного(-ых) лица (лиц), уполномоченного(-ых) подписывать документы юридического лица на совершение операций с деньгами и (или) иным имуществом;
- документ, выданный уполномоченным органом, подтверждающим факт прохождения государственной регистрации (перерегистрации) юридического лица;
- учредительные документы и (или) выписка из реестра держателей ценных бумаг;
- документы, удостоверяющие личность либо подтверждающие факт прохождения государственной регистрации (перерегистрации) учредителей (участников) юридического лица (за исключением документов учредителей (участников) акционерных обществ, а также хозяйственных товариществ, ведение реестра участников которых осуществляется единым регистратором), а также документы, удостоверяющие личность бенефициарных собственников юридического лица (за исключением случаев, когда бенефициарный собственник является учредителем (участником) юридического лица и выявлен на основании выписки из реестра акционеров (участников);
- документы, подтверждающие полномочия должностного(-ых) лица (лиц) лиц, на совершение действий от имени клиента без доверенности, в том числе на подписание документов юридического лица на совершение операций с деньгами и (или) иным имуществом;
- документ, удостоверяющий адрес места нахождения юридического лица;
- разрешение (в случае если деятельность клиента осуществляется посредством лицензирования или разрешительной процедуры в соответствии с Законом Республики Казахстан "О разрешениях и уведомлениях")

ДЛЯ ИНДИВИДУАЛЬНЫХ ПРЕДПРИНИМАТЕЛЕЙ

- документ, удостоверяющий личность;
- документ, выданный уполномоченным органом, подтверждающий факт прохождения государственной регистрации;
- Нотариально заверенная доверенность на право подписи Договора уполномоченным лицом в случае, если Договор не подписывается индивидуальным предпринимателем.

**все документы должны быть предоставлены в виде оригиналов либо нотариально засвидетельствованных копий документов, либо копий документов с проставлением апостиля или в легализованном порядке, установленном международными договорами, ратифицированными Республикой Казахстан.*

3.4. Платежная услуга оказывается на основании Договора, заключенного между Организацией и Мерчантом, который содержит следующие существенные условия:
- 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 поставщик платежных услуг оставляет за собой право на отказ в оказании платежной услуги;
- Порядок регулирования вопросов по несанкционированным платежным услугам;
- Право клиента 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.

Организация обеспечивает ознакомление Мерчанта с условиями Договора на казахском или русском языках.

3.5. Интеграция Мерчантов с АПК Организации:
- Мерчант предоставляет Организации IP-адреса тестового и боевого серверов;
- Организация предоставляет Мерчанту доступ к тестовой среде и API-документацию;
- Мерчант интегрируется с АПК организации;
- Мерчант и Организация проводят тестирование;
- В случае успешного прохождения предыдущего этапа, Организация предоставляет Мерчанту доступ к боевой среде.

3.6. Взаимодействие Держателя платежной карты и Мерчанта с Организацией:

1) Держатель платежной карты взаимодействует с Организацией, осуществляя выбор необходимой ему услуги/товара из перечня услуг/товаров, предоставляемых Интернет-магазином, с учетом Способа Платежа.
2) Для осуществления оплаты проводится Авторизация в зависимости от выбранного Способа Платежа. При этом Авторизация может быть Одностадийной и Двухстадийной:
   - Одностадийная Авторизация – Операция оплаты, при которой вся сумма платежа сразу списывается с карт - счета Держателя платежной карты.
   - Двухстадийная Авторизация – Операция оплаты, при которой сумма платежа на первой стадии резервируется (холдируется) на счете, к которому выпущена Карта, а на второй стадии, после подтверждения Авторизации Мерчантом, списывается с указанной карты.
3) Мерчант по согласованию с Организацией выбирает наиболее удобный для себя вариант, если иное не устанавливается Организацией для данного конкретного Мерчанта. В случае проведения Двухстадийной Авторизации операции Мерчант должен осуществить завершение второй стадии в течение 15 календарных дней со дня проведения первой стадии Авторизации.
4) Перевод Банком денег на расчетный счет Мерчанта или на специальный (транзитный) счет Платежной организации, в зависимости от договорных условий между Мерчантом и Организацией, осуществляется после Обработки Операций, в срок, установленный Договором. При этом Процессинг Двухстадийной Авторизации проходит только после успешного завершения обеих стадий. При зачислении денежных средств на специальный

(транзитный) счет Платежной организации, Платежная организация передает в Банк, в котором открыт специальный (транзитный) счет, реестры с суммами перечисления в пользу Мерчантов, Банк осуществляет перевод в пользу Мерчантов в течение 3 (трех) рабочих дней с момента получения реестров от Платежной организации.

5) Порядок проведения Авторизации:
- Держатель платежной карты в специальной электронной форме с использованием имеющегося у него компьютера/мобильного телефона/иного электронного устройства вводит реквизиты Карты, используемой для Операции оплаты.
- По запросу Организации Держатель платежной карты вводит дополнительные данные в зависимости от используемой технологии повышения безопасности платежей, в соответствии с правилами МПС.
- Организация передает информацию об осуществлении Авторизации в соответствии с предоставленными Держателем платежной карты реквизитами – в соответствии с Правилами МПС и договорными условиями с Банком.
- Организация информирует Мерчанта о результате Авторизации – согласии с проведением Операции или отказе в проведении Операции.

6) В случае возврата/отказа Держателем платежной карты от Услуги, либо необходимости проведения отмены ранее осуществленной Операции оплаты, Мерчант инициирует проведение таких операций в ЛК.
7) Фиксация совершения операций осуществляется Организацией в электронном виде и хранится в АПК Организации.
8) Организация на периодической основе - один раз в сутки, осуществляет Обработку Операций, совершенных с момента предыдущего цикла Обработки Операций. При этом в случае, если для совершения Авторизации был использован Способ Платежа – Двухстадийная Авторизация, Организация осуществляет Обработку Операций в отношении таких Авторизаций только после получения от Мерчанта запроса (так называемое «завершение авторизации»), подтверждающего необходимость Обработки Операции.
9) По результатам Обработки Операций Организация направляет Мерчанту Отчет по успешно прошедшим транзакциям.

3.7. **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 → Перевод платежа на расчетный счет Мерчанта/ специальный счет платежной организации → в случае если перевод платежа был осуществлен на специальный счет платежной организации, то → Платежная организация направляет реестр поручений на перевод в расчетный банк → Расчетный банк осуществляет перевод в пользу Мерчанта.

4. Стоимость платежных услуг (тарифы)

4.1. Виды, размер, порядок взимания комиссий и вознаграждений 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 (агентам, субагентам, поставщикам услуг, лицам, обеспечивающим технологическое взаимодействие с Платежной организацией при оказании последними платежных услуг и пр.).

4.2. Перечень тарифов, также, как и размер комиссий, вознаграждений не является фиксированным и может быть изменен, дополнен или отменен Платежной организацией в одностороннем порядке с обязательным согласованием с контрагентами, с обязательным уведомлением последних.

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

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

4.5. Платежная организация при оказании платежных услуг, в том числе через платежных агентов, субагентов обеспечивает ознакомление Клиентов/Держателей платежных карт с размером взимаемой комиссии до осуществления платежа, в денежном выражении.

4.6. **Тарифы**:

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 оплачиваются Мерчантом или Держателем платежной карты согласно действующим Тарифам:

- Комиссия/вознаграждение с каждой транзакции за обработку Операций по картам Visa и Mastercard и др. МПС – от 0% до 10%.
- Организация может установить минимальную комиссию/вознаграждение в денежном выражении, вне зависимости от процентной ставки.

4.7. Организация вправе предоставлять отдельным Мерчантам индивидуальные условия к утвержденным Тарифам, при этом условия варьируются, в зависимости от категории Мерчанта.

5. Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг

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

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

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

5.2. Порядок взаимодействия при работе с поставщиками услуг.

1) Лицом, ответственным за коммерческие вопросы Платежной организации, выявляется потребность физических лиц – резидентов РК по оплате сервисов Поставщиков услуг (в том числе, являющихся нерезидентами Республики Казахстан).

   Лицом, ответственным за коммерческие вопросы, проводятся маркетинговые исследования, включающие в себя анализ рынка, конкурентоспособности, потребительскую способность.

2) Также, лицом ответственным за коммерческие вопросы проводится экономическое обоснование включения нового Поставщика услуг в систему Платежной организации, а также выявляется платежная нагрузка на Клиентов.

3) После проведения вышеуказанных действий и принятия положительного решения по согласованию с лицом ответственным за финансовые вопросы об установлении деловых отношений с Поставщиком услуг, лицо ответственное за коммерческие вопросы проводит необходимые мероприятия в целях установления деловых отношений с конкретным поставщиком услуг, у представителя которого запрашиваются все необходимые документы в рамках ПОД/ФТ, предварительно оговариваются коммерческие условия по размерам комиссий, техническом взаимодействии и т.д., а также проводится анализ рисков в соответствии с внутренними документами Платежной организации.
4) В случае отсутствия комплаенс рисков производится обмен технической документацией для подключения Поставщика услуг к системе Платежной организации по протоколу технического взаимодействия API или подключения Платежной организации к системе Поставщика услуг.

5.3. Заключение договора с Поставщиком услуг.
1) После осуществления действий, определенных п.5.2 настоящих Правил между Платежной организацией и Поставщиком услуг заключается Договор.
2) Платежной организацией заключается агентский договор с Поставщиком услуг об оказании платежных услуг (договор поручения) с обязательным наделением правом Платежной организации о принятия платежа в пользу Поставщика услуг.
3) Принимая во внимание, если стороны договора являются резидентами различных государств, стороны проводят согласование положений договора, с учетом требований законодательств обеих сторон.
4) Поставщик услуг проходит регистрацию в Системе, с присвоением ID.
5) Платежная организация обязана передавать Поставщику услуг данные о каждом принятом платеже для внесения изменений в лицевой счет клиента. Сведения должны быть переданы непосредственно в период приема платежа на основании данных, указываемых клиентом, без ошибок и искажений.
6) При приеме платежей Платежной организацией взимается комиссия с платежа. Размер комиссии устанавливается Платежной организацией, и определяется условиями работы с поставщиками услуг.

6. Сведения о Системе управления рисками

6.1. Под системой управления рисками понимается комплекс мероприятий и способов снижения вероятности возникновения неблагоприятных последствий для бесперебойности функционирования АПК Организации в том числе, идентификация и предотвращение Мошеннических транзакций.
6.2. Система управления рисками утверждается исполнительным органом Организации.
6.3. В целях организации деятельности по управлению рисками Irbis Tech разрабатывает и утверждает внутренние документы в области управления рисками. Внутренние документы могут детализировать принципы управления рисками, а также содержать дополнительные мероприятия и способы управления рисками.
6.4. Irbis Tech предоставляет документ в области управления рисками по запросу Мерчантов и/или уполномоченных органов.
6.5. К функциям Мерчантов в части управления рисками относится:
6.5.1. соблюдение законодательства о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, при взаимодействии между Irbis Tech и Мерчантами в связи с оказанием им платежных услуг;
6.5.2. самостоятельное осуществление управления всеми рисками, присущими данному виду деятельности, при этом Мерчанты несут ответственность за последствия реализации указанных рисков.
6.6. Система управления рисками включает следующие мероприятия:
6.6.1. доведение до органов управления Irbis Tech соответствующей информации о рисках;
6.6.2. определение методик анализа рисков в Irbis Tech;
6.6.3. определение порядка обмена информацией, необходимой для управления рисками;

6.6.4. определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев;
6.6.5. определение порядка изменения операционных и технологических средств и процедур;
6.6.6. определение порядка оценки качества функционирования операционных и технологических средств, информационных систем независимой организацией;
6.6.7. определение порядка обеспечения защиты информации в Irbis Tech.

6.7. Способы управления рисками.

6.7.1. Способы управления рисками определяются Irbis Tech с учетом особенностей Организации, модели управления рисками, процедур расчета, количества и сумм проведенных транзакции, периода активности Мерчанта.
6.7.2. Мониторинг рисков транзакций осуществляется в режимах онлайн и офлайн.
6.7.2.1. Меры контроля в режиме онлайн принимаются для обеспечения, во время обработки запросов на авторизацию, приостановления или отклонения транзакций, соответствующих внутренним критериям Irbis Tech относительно минимальных требований к мониторингу рисков в отношении транзакций, а также дополнительным критериям на основе информации, собранной Организацией, касательно общих характеристик потенциально рисковых транзакций.
6.7.2.2. Другие транзакции, которые не были приостановлены или отклонены в процессе их осуществления, ввиду отсутствия прямого соответствия указанным критериям, подлежат обработке в режиме офлайн путем проведения дополнительного анализа в соответствии с внутренними критериями, относительно минимальных требований к мониторингу рисков в отношении транзакций, а также рассмотрения любой другой информации (известной Организации) о транзакции на предмет наличия ранее не выявленной потенциальной транзакции (процесс разработки параметров новых рисков, обеспечивающий улучшение процесса мониторинга рисков в отношении транзакций и корректировку с учетом изменений окружающей среды).
6.7.3. Irbis Tech проводит мониторинг рисков в соответствии с параметрами риска, предусмотренными Международной платежной системой, критериями Закона Республики Казахстан «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма» и собственными утвержденными параметрами риска.
6.7.4. Irbis Tech обеспечивает надлежащий мониторинг качества Операций, если для ввода данных карты (включая имя держателя карты, указанное на карте, номер карты, срок действия карты и код безопасности карты или CVV) для авторизации держателем карты используется экран для ввода данных Irbis Tech вместо системы Мерчанта с последующей повторной отправкой информации Irbis Tech, а также при условии получения Irbis Tech дополнительной информации в следующем минимальном объеме:
- IP-адрес держателя карты;
- Адрес электронной почты держателя карты;
- Описание операции;
- URL-адрес Мерчанта.

6.7.5. Irbis Tech регулярно отслеживает и, при необходимости, выполняет индивидуальную проверку транзакций/операций, которые вызывают серьезные сомнения относительно законности их проведения.
6.7.6. Другие способы управления рисками, предусмотренные Правилами и условиями договоров с Мерчантами, в том числе: анализ и изучение финансовой отчетности, других сведений и документов Мерчантов, а также анализ и изучение информации в средствах массовой информации, отслеживание и фиксирование параметров функционирования Мерчантов, соблюдение порядка расчетов.
6.8. Система управления рисками характеризуется такими элементами как мероприятия и способы управления.

Мероприятия по управлению рисками:

1) определение организационной структуры управления, обеспечивающей контроль за выполнением Мерчантами и другими третьими лицами требований к управлению рисками, установленных правилами управления рисками Платежной организации;
2) определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;

3) доведение до руководящего состава Платежной организации соответствующей информации о рисках;
4) определение показателей бесперебойности функционирования АПК Платежной организации, Системы электронных денег;
5) определение порядка обеспечения бесперебойности функционирования АПК Платежной организации, Системы электронных денег;
6) определение порядка обмена информацией, необходимой для управления рисками;
7) определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев; определение порядка изменения операционных и технологических средств и процедур;
8) определение порядка оценки качества функционирования операционных и технологических средств, информационных систем;
9) определение порядка обеспечения защиты информации в Платежной организации.

6.9. Способы управления рисками в Платежной организации определяются с учетом особенностей деятельности Платежной организации, модели управления рисками, процедур платежного клиринга и расчета, количества платежей и их сумм, времени окончательного расчета.

6.10. Способы управления рисками:
1) установление предельных размеров (лимитов) обязательств агентов и субагентов Платежной организации с учетом уровня риска;
2) осуществление расчета в пределах предоставленных Эмитентам денежных средств;
3) автоматизированное управление очередностью исполнения распоряжений/указаний Клиентов;
4) осуществление расчетов в соответствии с установленным в Договорах порядком;
5) использование безотзывных банковских гарантий;
6) другие способы управления рисками.

6.11. Irbis Tech принимает все предусмотренные законодательством меры по противодействию легализации и отмыванию доходов, полученных преступных путем, и финансированию терроризма, а также вправе устанавливать дополнительные меры и применять дополнительные санкции в отношении Мерчантов/Агентов/Клиентов в случаях наличия подозрений, что осуществляемая операция может быть связана с легализацией доходов и/или финансированием терроризма.

6.12. Irbis Tech в целях соблюдения требований законодательства в сфере противодействия легализации доходов, полученных преступным путем и финансированию терроризма и осуществления надлежащей проверки операций вправе блокировать операции на срок до 10 (десяти) рабочих дней без объяснения причины.

6.13. Irbis Tech вправе отказать в оказании Услуг любому лицу, если в отношении такого лица имеются данные, что оно связано и/или подозревается в связи с лицами, осуществляющими действия по легализации доходов, полученных преступным путем и/или финансированию терроризма, и/или осуществляет и/или подозревается в осуществлении деятельности, направленной на легализацию доходов и/или финансирование терроризма.

7. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами

7.1. В случае возникновения у Клиента/Мерчанта/Держателя платежной карты каких-либо претензий к Платежной организации по любой спорной ситуации, связанной с оказанием платежных услуг, Клиент/Мерчант/Держатель платежной карты обязан направить Платежной организации соответствующую претензию в письменной форме.

7.2. Клиент/Мерчант/Держатель платежной карты обязан 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: 050057, Республика Казахстан, г. Алматы, улица Жарокова 217;

2) путем личного обращения в офис платежной организации и ее нарочным предоставлением по адресу: 050057, Республика Казахстан, г. Алматы, улица Жарокова 217.

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

7.3. Обращения Клиентами/Мерчантами/Держателями платежной карты в службу технической поддержки Организации по телефону, направления сообщений через форму обратной связи на Сайте Организации не могут быть признаны обращением к Платежной организации с претензией и (или) расцениваться как досудебное урегулирование споров.

7.4. Ко всем претензиям, направляемым плательщиками Платежной организации, должны быть приложены надлежащим образом оформленные копии документов, подтверждающие факты, указанные в Заявлении. При этом Платежной организацией могут быть запрошены дополнительные сведения и (или) документы для всестороннего изучения спорной ситуации.

7.5. Платежная организация рассматривает полученную Претензию и подготавливает ответ в срок не более 30 (тридцати) календарных дней со дня получения соответствующей претензии.

7.6. Для надлежащего рассмотрения претензии 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/Мерчанта/Держателя платежной карты дополнительно документы (или их копии), объяснения и иные сведения. По запросу Платежной организации Клиент/Мерчант/Держатель платежной карты 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 плательщика;
- подготавливает мотивированный письменный ответ Клиенту/Мерчанту/Держателю платежной карты на претензию и направляет ответ по адресу, указанному в претензии.

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

7.8. В случае, если Мерчанту необходимо осуществить Операцию, и это невозможно осуществить в рамках стандартного порядка взаимодействия, описанного в настоящих Правилах (например, в случае сбоев в работе систем, обнаружения ошибочных операций и т.п. спорных ситуаций), Мерчант направляет в отсканированном виде в Irbis Tech запрос на адрес электронной почты Irbis Tech на обработку такой Операции: Поручение о возврате средств (если необходимо осуществить Операцию возврата) или гарантийное письмо (для других видов Операций) в свободной форме или в форме, установленной в Договоре между Организацией и Мерчантом.

7.9. Мерчант может осуществить Операцию возврата/отмены через Личный кабинет, если на момент осуществления Операций имеется техническая возможность, при этом Поручение о возврате средств и/или Гарантийное письмо не оформляются.

7.10. Irbis Tech рассматривает полученный от Мерчанта запрос и, при наличии возможности, осуществляет проведение запрошенной Операции. Такая Операция в дальнейшем проходит Обработку операций аналогично всем прочим Операциям.

8. Порядок соблюдения мер информационной безопасности

8.1. **Основы обеспечения информационной безопасности Платежной организации**

1) **Информационная безопасность** предполагает состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз. Система обеспечения информационной безопасности Платежной организации – эффективный инструмент защиты интересов собственников и пользователей информации. Следует отметить, что ущерб может быть

нанесен не только несанкционированным доступом к информации. Он может быть получен в результате поломки коммуникационного или информационного оборудования.

2) **Защита информации** включает полный комплекс мер по обеспечению целостности и конфиденциальности информации при условии ее доступности для пользователей, имеющих соответствующие права.

Целостность – понятие, определяющее сохранность качества информации и ее свойств.

Конфиденциальность предполагает обеспечение секретности данных и доступа к определенной информации отдельным пользователям.

Доступность – качество информации, определяющее ее быстрое и точное нахождение конкретными пользователями.

Цель защиты информации – минимизация ущерба вследствие нарушения требований целостности, конфиденциальности и доступности.

Термин «безопасность информации» описывает ситуацию, исключающую доступ для просмотра, модерации и уничтожения данных субъектами без наличия соответствующих прав. Это понятие включает обеспечение защиты от утечки и кражи информации с помощью современных технологий и инновационных устройств.

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

- определения целей и задач по обеспечению информационной безопасности;
- определения направлений для развития системы обеспечения информационной безопасности.

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

- гарантирование использования по назначению компьютеров и телекоммуникационных ресурсов Платежной организации, ее сотрудниками, независимыми подрядчиками и другими пользователями;
- выявление, реагирование (противодействие атакам в реальном времени), разрешение и анализ причин возникновения инцидентов информационной безопасности;
- управление доступом к активам;
- антивирусная защита;
- резервное копирование данных;
- управление непрерывностью бизнеса;
- регистрация, анализ и контроль событий информационной безопасности;
- выявление уязвимостей в информационных системах платежной организации, с использованием которых могут быть реализованы угрозы информационной безопасности;
- формирование принципов внесения изменений, процедуры установки, модификации и технического обслуживания информационных систем платежной организации;
- физическая безопасность активов;
- защита сетевого периметра;
- соблюдение условий всех программных лицензий, авторских прав и законов, касающихся интеллектуальной собственности.

В рамках проверки деятельности по обеспечению информационной безопасности осуществляются внутренний и внешний (независимый) контроль/аудит информационной безопасности.

В рамках совершенствования деятельности по обеспечению информационной безопасности осуществляются анализ результатов функционирования системы обеспечения информационной безопасности платежной организации.

8.2. Обязательства по обеспечению общей безопасности платежных услуг, защиты передаваемых данных и информации несет Организация.

8.3. Irbis Tech обязуется соблюдать конфиденциальность в отношении всех переданных ему Мерчантами данных, а также данных, ставших ему известными в ходе исполнения обязательств при оказании платежных услуг, за исключением случаев, предусмотренных Правилами и/или законодательством Республики Казахстан, а также случаев, когда такая информация является общеизвестной или раскрыта по требованию или с разрешения Мерчанта или иного получателя платежных услуг.

8.4. Мерчант обязуется незамедлительно уведомлять Irbis Tech о любых операциях, произведенных без его согласия. В случае непредоставления соответствующего уведомления в течение календарных суток с момента осуществления операции и направления Irbis Tech соответствующего уведомления, операция считается осуществленной Мерчантом.

8.5. Процедуры безопасности

8.5.1. Предоставление платежных услуг производится в соответствии с процедурами безопасности, установленными настоящими Правилами, Договором и Требованиями об информационных и технологических средствах, системах безопасности, механизмах и системах контроля, необходимых для оказания платежных услуг, утвержденными в Организации.

8.5.2. Irbis Tech при оказании платежных услуг осуществляет сбор и обработку персональных данных с согласия субъекта персональных данных, за исключением случаев, предусмотренных Законом Республики Казахстан «О персональных данных и их защите».

8.5.3. Процедуры безопасности обеспечивают:

1) правомерность на получения соответствующих платежных услуг;
2) выявление наличия искажений и (или) изменений в содержании электронных документов, на основании которых клиенту предоставляются услуги;
3) защиту от несанкционированного доступа к информации и целостность данной информации и полную сохранность информации в электронных архивах и базах данных.

8.5.4. Операция является санкционированной, если она произведена лицом, которое имело полномочия совершить операцию, и не противоречит законодательству Республики Казахстан, а также при условии, если указание принято банком отправителя денег с соблюдением установленного порядка защитных действий от несанкционированных платежей.

8.5.5. Предоставление Услуг является санкционированным в случае выполнения клиентом процедур безопасности, установленных настоящими Правилами и Договором.

8.5.6. Несанкционированной является операция, осуществленная без соблюдения требований, установленных законодательством, а также с использованием поддельных платежных инструментов.

8.5.7. В качестве элементов защитных действий используются идентификационные коды, шифрование и иные способы защиты, не противоречащие законодательству Республики Казахстан.

8.5.8. Irbis Tech осуществляет мониторинг за соблюдением Клиентами/Мерчантами требований к защите информации, определенных Договором и настоящими Правилами.

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

9.1. Порядок соблюдения мер информационной безопасности

Участники Системы обязуются соблюдать конфиденциальность в отношении не являющихся общедоступными сведений о других Участниках Системы, ставших известными Участникам Системы в связи с присоединением к настоящим Правилам, за исключением случаев, когда информация:

• раскрыта по требованию или с разрешения Клиента Системы, являющегося Владельцем данной информации;

• подлежит предоставлению третьим лицам в объеме, необходимом для исполнения обязательств, предусмотренных настоящими Правилами;

• требует раскрытия по основаниям, предусмотренным законодательством Республики Казахстан.

Не является нарушением конфиденциальности и безопасности Участников Системы предоставление конфиденциальной информации третьей стороне в целях исполнения Правил и иных соглашений Участников Системы; предоставление конфиденциальной информации по

законному требованию правоохранительных и иных уполномоченных государственных органов, а также в других предусмотренных действующим законодательством Республики Казахстан случаях.

Аутентификация Клиента Системы при доступе к Системе осуществляется программным обеспечением Системы с использованием авторизационных данных Клиента Системы: логина, пароля, электронной почты и двухэтапной аутентификации.

Оператор 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.

Оператор обеспечивает защиту информации о средствах и методах обеспечения информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Республики Казахстан, которая может стать ему известной в ходе осуществления деятельности в Системы.

Участники Системы обязуются принимать все необходимые меры для обеспечения безопасности и по защите информации и документов, обмен которыми осуществляется в Системе или которые доступны Участникам Системы в связи с использованием Системы, а также с целью выявления (предотвращения) мошенничества и противодействия легализации доходов, полученных преступным путем, и финансированию терроризма.

Средства и меры предотвращения несанкционированного доступа к программно-техническим средствам, применяемые в Системе, включая программно-технические средства защиты, должны обеспечивать уровень защиты информации и сохранение ее конфиденциальности в соответствии с требованиями, установленными законодательством Республики Казахстан. Участники Системы обязуются принимать все необходимые меры по сохранению конфиденциальности, предотвращению несанкционированного использования и защите идентификационных данных от несанкционированного доступа со стороны третьих лиц.

В случае утраты авторизационных данных Клиентом, Оператор предоставляет Клиенту возможность восстановления доступа к Системе путем подачи Клиентом соответствующего заявления по установленной Оператором форме на интернет-ресурс Оператора.

Серверная структура:

Сервис разработан на серверной технологии PYTHON и использует для работы PYTHON версии 3.8.2+, запущенный в режиме WSGI. В качестве системы хранения данных используется MySQL Server версии 8.0.27. Серверная структура системы состоит из: ISP Gate, DMZ Gate, vlan DMZ 100, load balancing server, 2 nodes, Front End (static media, js, react), Back End (PYTHON сервер), DB cluster (MySQL). Также организован сервер баз данных, который обеспечивает создание и хранение бекапов. Все серверы работают под управлением CentOS 7.

Список зависимостей:

certifi==2021.5.30, chardet==4.0.0, coreapi==2.3.3, coreschema==0.0.4, Django==2.2, django-admin-rangefilter==0.8.1, django-background-tasks==1.2.5, django-cleanup==5.2.0, django-compat==1.0.15, django-cors-headers==3.7.0, django-exclusivebooleanfield==0.3.0, django-filter==2.1.0, django-jet==1.0.8, django-static-jquery-ui==1.12.1.1, djangorestframework==3.9.0, djangorestframework-jwt==1.11.0, drf-nested-routers==0.91, drf-yasg==1.13.0, idna==2.10, inflection==0.5.1, itypes==1.2.0, Jinja2==3.0.1, MarkupSafe==2.0.1, Pillow==8.4.0, PyJWT==1.7.1, pyotp==2.6.0, pytz==2021.1, qrcode==7.3.1, requests==2.25.1, ruamel.yaml==0.17.7, ruamel.yaml.clib==0.2.2, six==1.16.0, sqlparse==0.4.1, uritemplate==3.0.1, urllib3==1.26.5

Отказоустойчивость:

Отказоустойчивость сервиса обеспечивается за счет распределения нагрузки между двумя серверами приложений. Эту функцию выполняет программное обеспечение Nginx версии 1.8, которое выступает в роли frontend-сервера, проксирующего запросы к серверам приложений в режиме round-robin. В случае недоступности одного из серверов (падение канала связи, высокая текущая нагрузка, выход сервера из строя) все запросы автоматически и без задержек на переключение перенаправляются на сервер, оставшийся в онлайн-режиме. Таким образом достигается баланс производительности серверов в базовом режиме работы и обеспечение бесперебойной обработки транзакций в случае непредвиденных обстоятельств, когда один из серверов по каким-либо причинам временно выходит из строя. Сервер баз данных работает в режиме репликации Master-Slave с резервным сервером, и в случае отказа работы основного сервера ноды обработки транзакций автоматически переключаются на резервный.

Резервное копирование:

Резервное копирование сервера баз данных осуществляется встроенными средствами MySQL с сохранением бекапов на резервном сервере баз данных в течение одного месяца. Схема копирования такова: каждый час + финальное в 1:00 с удалением ежечасных копий + журнал транзакций, что позволяет восстанавливать все транзакции независимо от того в какой момент после бекапа произошел сбой. Бекапы старше одного месяца удаляются в целях недопущения переполнения хранилища данных. Актуальность и сохранение кодовой базы системы обработки транзакций обеспечивается системой управления версиями на базе Git. Непосредственно репозитории кода хранятся на внутренних серверах http://10.0.42.10/Ramzes/cepheus-admin/-/blob/master, деплоймент с которого, в случае отказа серверов, может быть произведен в кратчайшие сроки.

Безопасность доступа к серверной инфраструктуре:

Административный доступ к любому из серверов возможен только при наличии 2048-битного SSH2-RSA-ключа. Получить доступ к серверной инфраструктуре перебором паролей или любым другим несанкционированным способом невозможно. Доступ клиента в личный кабинет, как и доступ администратора системы в кабинет управления транзакциями, осуществляется только посредством двухфакторной авторизации, которая предоставляется сервисом forticlient. Для прохождения авторизации с помощью данного сервиса необходимо иметь установленное в браузер расширение, либо мобильное приложение. Авторизация на этом участке при помощи других, менее защищенных методов невозможна. Доступ администратора происходит через защищённое соединение с двухфакторной аутенфикацией, далее вводится ключ доступа на сервер.

CyberSource

Каждая транзакция в сервисе системы проходит через фильтр CyberSource. Данный фильтр является высокоэффективной мерой защиты безопасности транзакций и обеспечивает высокий уровень защиты от мошенничества. CyberSource не требует наличия включенного 3DSecure или другого метода защиты безопасности транзакций, что позволяет сервису системы значительно расширить пользовательскую базу плательщиков за счет абонентов, не имеющих или не включающих 3DSecure.

Trustkeeper

Серверная инфраструктура системы периодически подвергается сканированию на уязвимости при помощи сервиса Trustkeeper. Во время тестирования серверы подвергаются эмуляции современных видов атак, использования новых уязвимостей и методов проникновения. Данная процедура позволяет своевременно выявлять и устранять проблемы с обеспечением безопасности.

Антифрод:

Все транзакции по платежным картам после передачи из сервиса системы в платежную систему банка подвергаются обработке антифрод-фильтром. На основе набора правил, таких как наличие маски карты в продаже на черном рынке, степень благонадежности IP-адреса, с которого совершается транзакция, использование TOR-клиента и пр., фильтр рассчитывает степень риска транзакции и присваивает ей определенный рейтинг. В зависимости от установленного у мерчанта уровня надежности транзакций, система банка обрабатывает или отвергает транзакцию.

Описание программно-технических средств:

- бесперебойное интернет-соединение;
- персональный компьютер, защищенный VPN соединением;
- доступ к программному обеспечению системы.

Требования к программно-техническим средствам:

- WINDOWS Desktop 7;
- Linux Ubuntu Desktop 17.10 / Debian Desktop 10.12;
- IOS Desktop (последняя установленная версия не младше 3-х лет);
- Программное обеспечение на базе Android / IOS не младше 3-х лет;

Аппаратное обеспечение:
Название модели: MacBook Pro
Идентификатор модели: MacBookPro18,1
Чип: Apple M1 Pro
Общее количество ядер: 10 (8 производительности и 2 эффективности)
Память: 16 ГБ
Версия системной прошивки: 7429.81.3
Версия загрузчика ОС: 7429.81.3;

Имя устройства: DESKTOP-12LE9UJ
Процессор: AMD Ryzen 5 5600H with Radeon Graphics 3.30 GHz
Оперативная память:16,0 ГБ
Код устройства: 6CC1291D-C887-4BC4-A1FA-3C3612DEEDAE
Код продукта: 00330-80000-00000-AA055
Тип системы: 64-разрядная операционная система, процессор x64;

Servers: Lenovo x3550 m5
CPU: Intel E5-2648L v3
RAM: Lenovo 46W0796
SAN: Lenovo Storewize v5000
Virtualization: Microsoft Hyper-V 2016 Datacenter.

10. ***Отправка сообщений в антифрод-центр.***

10.1. При выявлении мошеннических транзакций Клиента, ТОО «Irbis Tech» обязано проводить мероприятия, описанные в Статье 25-1 Закона «О платежах и платежных системах», а именно:

1) приостанавливает транзакцию и (или) блокируют сумму денег на срок не более трех рабочих дней;
2) предоставляет клиенту информацию о приостановлении транзакции и (или) блокировании платежа и (или) перевода денег с указанием причин и оснований;
3) в течение 3 (трех) рабочих дней проводит предметный (детальный) анализ по деятельности и (или) операции своего клиента, в том числе по получению дополнительной информации от клиента для выяснения обстоятельств и принятия решения;
4) в случае подтверждения оснований (подозрений) об участии клиента в платежных операциях, связанных с платежной транзакцией с признаками мошенничества, направляет сообщение оператору антифрод-центру.
5) направляет уведомление в антифрод-центр для отправки информации по платежной транзакции с признаками мошенничества в орган уголовного преследования для последующего проведения мероприятий, установленных законами Республики Казахстан;
6) в случае неполучения по истечении трех рабочих дней решения органа уголовного преследования о дальнейшем приостановлении платежа и (или) перевода денег либо об отсутствии необходимости в приостановлении такого платежа и (или) перевода денег осуществляет данную транзакцию, если не имеется иных оснований, предусмотренных законами Республики Казахстан, препятствующих проведению данного платежа и (или) перевода денег.

10.2. Транзакция признается Iribis Tech мошеннической, если:

1) имеется заявление клиента о выявлении им транзакции с признаками мошенничества;
2) имеется подтвержденная информация от органа уголовного преследования;
3) в соответствии с внутренними документами Irbis Tech имеются такие основания;
4) бенефициар транзакции находится в базе данных о событиях и попытках осуществления платежной транзакции с признаками мошенничества.

10.3. В случае получении информации от антифрод-центра о лицах, связанных с платежными транзакциями с признаками мошенничества, Irbis Tech отказывает в проведении или приостанавливает транзакцию в сроки и порядке, определенном нормативным правовым актом Национального Банка Республики Казахстан.

10.4. Irbis Tech отказывает в осуществлении транзакции при совпадении информации о бенефициаре транзакции с информацией о бенефициаре, имеющейся в базе о событиях, подтвержденной органом уголовного преследования. При отказе в проведении транзакции, Irbis Tech предоставляет клиенту – отправителю денег информацию об отказе в проведении транзакции с указанием причин и оснований.
В случае, если клиент отправитель денег принимает все риски, Irbis Tech возобновляет данную транзакцию в пользу бенефициара, включенного в базу о попытках.
Если клиент не принимает риски и не желает продолжить транзакцию, Irbis Tech отклоняет данную транзакцию.

10.5. Сообщение о платежной транзакции с признаками мошенничества направляется в электронной форме и содержит реквизиты для идентификации клиента по форме, установленной внутренними документами оператора антифрод-центра, но не ограничиваясь следующими реквизитами при осуществлении транзакции с использованием:
1) банковского счета: номер счета, сумма и время платежной транзакции;
2) платежной карточки: номер карточки и (или) уникальный идентификатор платежной транзакции (при наличии), присваиваемый эквайером в процессе ее обработки, сумма и время платежной транзакции;
3) электронного кошелька электронных денег: реквизиты кошелька, сумма и время платежной транзакции.

10.6. Организация выявляет платежную транзакцию с признаками мошенничества, но не ограничиваясь ими, на основании следующих критериев (признаков), утвержденных внутренними документами:
1) несоответствие характера (нетипичных) проводимой клиентом операции, выявленных организацией на основе анализа по обычно совершаемым операциям (осуществляемой клиентом деятельности), в частности:
время (дни) осуществления операции;
место осуществления операций (физические нахождение клиента, место осуществления операции и так далее);
устройство, с использованием которого осуществляется операция;
2) несоответствие параметров проводимой клиентом операции:
сумма операции;
периодичность (частота) осуществления операций;
получатель (бенефициар) денег;
3) несоответствие объема проводимых клиентом операций:
в пользу иностранных поставщиков услуг, в том числе платформ цифровых активов;
в пользу поставщиков товар, работ и услуг, деятельность не связана с приемом крупных платежей.

11. ***Заключительные положения***

11.1. Настоящие Правила утверждены Решением единственного участника ТОО «Irbis Tech» и вступают в силу с даты, указанной в настоящих Правилах. Изменения и дополнения в Правила могут быть внесены по решению Участника ТОО «Irbis Tech», и подлежат обязательному направлению в уполномоченный орган в порядке и сроки, предусмотренные нормативными правовыми актами уполномоченного органа.

11.2 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.