

Утверждаю

Директор ТОО «Payment Processing»

«08» декабря 2020 г.



ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ

ТОО «Payment Processing»

АЛМАТЫ - 2020г.

Оглавление

1. Общие положения.....	3
2. Описание платежных услуг	5
3. Порядок и сроки оказания платежных услуг.....	6
4. Стоимость платежных услуг (тарифы)	16
5. Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией.	16
6. Сведения о Системе управления рисками	18
7. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами	21
8. Порядок соблюдения мер информационной безопасности	22

1. Общие положения

1.1. Настоящие Правила осуществления деятельности платежной организации ТОО «Payment Processing» (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 «Payment Processing» и определяют порядок деятельности организации ТОО «Payment Processing» в качестве платежной организации.

1.2. Термины и определения

Авторизация – процедура запроса и последующего получения Мерчантом от ТОО «Payment Processing» 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 со счета Покупателя.

Двустадийная Авторизация – Операция оплаты, при которой сумма платежа на первой стадии резервируется (холдингуется) на счете, к которому выпущена Платежная карточка Покупателя, а на второй стадии, после подтверждения Авторизации Мерчантом, списывается с указанного счета Покупателя.

АПК – специализированный аппаратно-программный комплекс ТОО «Payment Processing», Банка.

Банк – банки второго уровня, с которым сотрудничает ТОО «Payment Processing».

Банк-эмитент – банки, осуществляющие выпуск Платежных карточек, в том числе Банк.

Банк-эквайер – Банк, обеспечивающий проведение Операций по Платежным карточкам.

Держатель Платежной карточки (Покупатель) – законный держатель Платежной карточки, использующий Платежную карточку для совершения Операций.

ЛК – личный кабинет Мерчанта, посредством которого Мерчант имеет возможность самостоятельно просматривать информацию об Операциях, инициировать проведение Операций возврата/отмены оплаты.

Мерчант – это предприятие торговли (услуг), где к оплате принимаются Платежные карточки.

Международные платежные системы VG (МИС) – международные платежные системы: Visa International и MasterCard International.

Обработка Операций (Процессинг) – обработка ТОО «Payment Processing» 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 Платежной карточки) информации по совершенным Операциям.

Операция (Операции) – общее определение, включающее в себя следующие виды операций: Операцию оплаты, Операцию отмены оплаты, Операцию возврата, Операцию отмены возврата.

Платежная карточка – банковская карта МПС.

Способ платежа – канал/способ осуществления Операции оплаты в Интернет-магазине с использованием Платежной карточки в качестве электронного средства платежа.

Транзакция – финансовая операция с Платежной карточкой, в результате которой производится оплата каких-либо товаров или услуг.

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

WEB-сайт Системы – WEB-сайт, размещенный в ИТС Интернет по электронному адресу: <https://ioka.kz/>.

Платежная организация – ТОО «Payment Processing», являющееся коммерческой организацией, которое в соответствии с Законом о платежах, правомочно осуществлять деятельность по оказанию платежных услуг.

Система по учету платежей (Система) – совокупность программно-технических средств, обеспечивающих информационно-технологическое взаимодействие и регистрацию платежей.

Аутентификационные данные – уникальные имя пользователя (login), пароль (password) и/или PIN-код и/или Код подтверждения привязки Пользователя, используемые для доступа к Системе из ИТС Интернет и/или через терминал и/или через мобильное приложение и совершения операций в пределах суммы денежных средств, доступной Пользователю в целях предъявления Эмитенту требований об осуществлении расчетов. Аутентификационные данные присваиваются Пользователю в момент регистрации Пользователя в Системе.

Пользователь – физическое лицо, обладающее надлежащей дееспособностью в соответствии с действующим законодательством РК для совершения Платежа, совершившее конклюдентные действия, направленные на заключение Договора об оказании услуг посредством акцепта условий Договора-оферты, и обладающее Аутентификационными данными для доступа к Системе для ее использования в целях управления Учетной записью Пользователя, осуществлению доступа к Электронным деньгам на Балансе Учетной записи Пользователя в целях совершения Платежей.

Код подтверждения – уникальная последовательность цифр, предоставляемая Пользователю Оператором Системы посредством SMS-сообщения или ТОО «Payment Processing» робота на Абонентский номер Пользователя, указанный им при регистрации в системе «ioka», в целях Подтверждения Платежа. Код подтверждения предоставляется Оператором Системы Пользователю для каждого Платежа в порядке, предусмотренном Оферты системы электронных денег ioka.

Учетная запись Пользователя – запись в аналитическом учете Оператора Системы, представляющая собой средство учета Электронных денег, как поступающих на Баланс Учетной записи Пользователя, так и расходуемых Пользователем на оплату Платежей. Идентификатором Учетной записи Пользователя в учете Оператора Системы выступает Абонентский номер Пользователя.

Шлюз – программное обеспечение для создания электронного канала посредством которого производится обмен данными транзакции и данными по запросу на Авторизацию между Мерчантом и Банком.

1.3. Платежная организация при наличии регистрационного номера учетной регистрации платежной организации, присвоенного Национальным Банком, (далее – регистрационный номер) 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.

2. Описание платежных услуг

2.1. 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 оказываются платежной организацией на основании договоров, заключенных с банком/банками второго уровня и «Payment Processing», при этом обеспечивается обработка платежей инициированных с использованием Платежных карточек с указанием реквизитов назначения соответствующего платежа и Мерчанта соответствующего платежа с последующим обеспечением передачи Платежной организацией реквизитов по платежу для его исполнения в адрес соответствующего банка, а банк в свою очередь исполняет указание клиента, переданное через платежную организацию в электронной форме и перечисляет платеж Мерчанту.

2.1.1. Схема приема платежей по Платежным карточкам

2.1.1.1. Клиент Мерчанта со страницы его сайта переходит на страницу оплаты Payment Processing.

2.1.1.2. Клиент Мерчанта вводит реквизиты Платежной карточки (тип Платежной карточки, имя держателя Платежной карточки, номер Платежной карточки, срок действия Платежной карточки, CVV).

2.1.1.3. Если Мерчант выбрал одностадийную схему проведения платежа, Payment Processing списывает сумму с Платежной карточки клиента Мерчанта.

2.1.1.4. Если Мерчант выбрал двустадийную схему проведения платежа:

1. Payment Processing блокирует сумму на Платежной карточке клиента Мерчанта.
2. Если Мерчант подтверждает операцию, то Payment Processing списывает сумму с Платежной карточки клиента Мерчанта.
3. Если Мерчант не подтверждает операцию, то Payment Processing не списывает сумму с Платежной карточки клиента Мерчанта.

2.1.2. Схема выплаты клиентам на Платежные карточки

2.1.2.1. Клиент Мерчанта на странице его сайта указывает сумму для выплаты.

2.1.2.2. Клиент Мерчанта переходит на страницу Payment Processing для ввода реквизитов Платежной карточки.

2.1.2.3. Клиент Мерчанта заполняет реквизиты Платежной карточки (имя держателя Платежной карточки, номер Платежной карточки).

2.1.2.4. Мерчант производит внутреннюю проверку запроса клиента на выплату.

2.1.2.4.1. Если Мерчант не подтвердил запрос, то Payment Processing не осуществляет выплату на Платежную карточку клиента Мерчанта.

2.1.2.4.2. Если Мерчант подтвердил запрос, то Payment Processing производит выплату на Платежную карточку клиента Мерчанта.

2.2. Платёжная организация в соответствии с требованиями действующего законодательства РК о платежах и платёжных системах не вправе оказывать услуги, указанные в пункте 2.1. настоящих Правил, через платёжных агентов и платёжных субагентов.

3. Порядок и сроки оказания платежных услуг

3.1. 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.

3.1.1. Условия получения Услуг

3.1.1.1. Для получения Услуг Payment Processing Мерчанту необходимо: иметь зарегистрированное юридическое лицо (либо статус индивидуального предпринимателя), работающий интернет-сайт и счет в любом банке второго уровня РК.

3.1.1.1. Способ № 1:

1) В рамках исполнения/оказания данной Услуги Payment Processing, в рамках договоров, заключенных с банком/ банками второго уровня, обеспечивает:

Прием платежей, инициированных с использованием Платежных карточек 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, переданное через программное обеспечение Платежной организации в электронной форме.

2) Инициация клиентом операций/платежей производится посредством 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 банковского счета клиента/Платежной карточки клиента, с их зачислением в пользу банка с целью последующего исполнения поручения/распоряжения клиента, полученного Платежной организацией от клиента и переданного Платежной организацией в банк.

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

- Клиент посредством сети интернет/мобильного телефона, заходит в соответствующее приложение Платежной организации;
- Клиент знакомится с тарифом/размером комиссии за предоставление Платежной организации соответствующей услуги;
- Клиент ознакомивается с условиями предоставления услуги и соглашается с условиями Договора-оферты, размещенными в соответствующем приложении;
- Клиент в приложении инициирует платеж в пользу банка;
- Клиент вводит в электронное приложение реквизиты для исполнения платежа банком;
- Для оплаты платежа клиент вводит реквизиты Платежной карточки;
- Платежная организация посредством запроса в банк инициирует распоряжение клиента полученного в электронной форме;

- Банк получив подтверждение от Платежной организации и клиента производит списание с Платежной карточки, и перевода Платежа в пользу Поставщика услуг, указанного в поручении Клиента, сумму инициируемой клиентом операции с учетом комиссионного вознаграждения Платежной организации.
- Платежная организация получает от банка подтверждение исполнения Операции;
- Платежная организация выдает клиенту электронный чек, подтверждающий совершение клиентом операции и списание с клиента комиссии Платежной организации.

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

Схема потока денежных средств и информационных потоков при оказании платежной услуги Способом № 1:



3.1.1.1.2. Способ № 2 (с использованием специального банковского счета):

- 1) В рамках исполнения/оказания данной услуги Платежная организация, в рамках договоров, заключенных с банком/ банками второго уровня, обеспечивает:

Прием платежей, инициированных с использованием Карточки Платежных карточек 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.

- 2) Инициация клиентом операций/ платежей производится посредством 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 карточки клиента, с их зачислением в пользу банка с целью последующего исполнения поручения/ распоряжения клиента полученного Платежной организацией от клиента и переданного Платежной организацией в банк.

- 3) При оказании услуги Платежная организация обеспечивает следующий алгоритм действий:

- Клиент посредством сети интернет/мобильного телефона, заходит в соответствующее приложение Банка;
- Клиент знакомится с тарифом/размером комиссии за предоставление соответствующей услуги;

- Клиент ознакливается с условиями предоставления услуги и соглашается с условиями Договора-оферты, размещенными в соответствующем приложении;
- Клиент в приложении инициирует платеж в пользу Поставщика услуг (Провайдера);
- Клиент вводит в электронное приложение реквизиты для исполнения платежа банком;
- Для оплаты платежа клиент вводит реквизиты Платежной карточки;
- Банк, получив подтверждение от Платежной организации и клиента производит списание с Платежной карточки Клиента, и переводит Платеж на специализированный (транзитный) счет Банка, сумму инициируемой клиентом операции.
- Платежная организация получает от банка подтверждение исполнения Операции;
- Банк или Платежная организация, в зависимости от договорных отношений, выдает клиенту электронный чек, подтверждающий совершение клиентом операции и списание с клиента комиссии.
- Платежная организация передает расчетному банку, в котором открыт этим банком специализированный (транзитный) счет, реестры в электронном виде, которые включают в себя, информацию о Платежах, с указанием реквизитов Платежей, сумм Платежей, а также реквизиты Получателя, после чего расчетный банк производит зачисление денежных средств Клиентов на расчетные счета Получателей.

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

Схема потока денежных средств и информационных потоков при оказании платежной услуги Способом № 2:



3.1.2. Стандартные этапы подключения к Payment Processing:

3.1.2.1. Заявка на подключение

На сайте <https://ioka.kz/> заявка на подключение содержит наименование и URL-адрес сайта Мерчанта, номер телефона и email представителя Мерчанта.

3.1.2.2. Требования к сайту Мерчанта

- a) URL-адрес и все внутренние ссылки сайта Мерчанта должны быть рабочими и адекватно обрабатываемыми.
- b) Сайт Мерчанта не должен предоставлять услуги «развлечений для взрослых» («Adult Entertainment»).
- c) 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.
- d) Сайт не должен располагаться на бесплатных серверах, предоставляющих услуги хостинга.
- e) 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.
- f) Перечень продаваемых товаров (работ, услуг), перечисленных в анкете Мерчанта, должен соответствовать перечню товаров (работ, услуг), предлагаемых на сайте.
- g) 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.
- h) Реквизиты Платежной карточки не должны приниматься на сайте. Для оплаты с использованием Платежной карточки клиент должен обязательно переадресовываться на АПК Payment Processing.
- i) Наличие на сайте описания процедур заказа товаров (работ, услуг) и их оплаты с использованием Платежной карточки. Также обязательным условием является наличие на сайте формы оплаты товара (работы, услуги) с использованием Платежной карточки и переадресация клиента на сайт АПК Payment Processing.
- j) 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 Платежной карточки.
- k) 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.
- l) Мерчант обязан предусмотреть осуществление контроля получения заказов клиентами.
- m) Мерчант обязан предусмотреть методы ограничения и контроля рисков мошеннических операций. Обязательным условием является применение при этом возможностей АПК Payment Processing по борьбе с мошенничеством.
- n) Все страницы, которые связаны с работой сайта, должны находиться под единым доменным именем.
- o) Наличие предупреждения о том, что посещение сайта, приобретение и доставка клиента конкретного товара (работы, услуги) могут быть незаконными на территории страны, где находится клиент.
- p) 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.

3.1.2.3. Пакет документов для подключения к Payment Processing

3.1.2.3.1. В соответствии с требованиями законодательства РК о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, в целях идентификации Мерчанта, с учетом установленных для платежных организаций обязательных требований к досье клиента, запрашивается соответствующая информация и документы о Мерчанте. Дополнительно могут быть затребованы иные информации и документы, в частности:

- о способах доставки Товара Покупателям;
- об источниках происхождения товаров;
- о наличии у Мерчанта сертификатов на предоставление предлагаемых Товаров, сертификатов соответствия, гигиенических и прочих сертификатов;
- об авторских правах на предлагаемые Товары.

3.1.2.4. Договор-оферта на оказание платежных услуг

3.1.2.4.1. Для надлежащей проверки и идентификации мерчантов и соблюдения требований Закона Республики Казахстан от 28 августа 2009 года № 191-IV «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма», перед установлением деловых отношений Payment Processing принимает следующие меры:

1) фиксирование сведений, необходимых для идентификации физического лица: данные документа, удостоверяющего его личность, индивидуальный идентификационный номер (за исключением случаев, когда физическому лицу не присвоен индивидуальный идентификационный номер в соответствии с законодательством Республики Казахстан), а также юридический адрес;

2) фиксирование сведений, необходимых для идентификации юридического лица (филиала, представительства): данные справки о государственной (учетной) регистрации (перерегистрации) юридического лица (филиала, представительства), бизнес-идентификационный номер (за исключением случаев, когда юридическому лицу не присвоен бизнес-идентификационный номер в соответствии с законодательством Республики Казахстан) либо номер, под которым юридическое лицо-нерезидент зарегистрировано в иностранном государстве, а также адрес места нахождения;

3) выявление бенефициарного собственника и фиксирование сведений, необходимых для его идентификации.

Фиксирование сведений, необходимых для идентификации бенефициарного собственника, осуществляется на основе информации и (или) документов, предоставляемых клиентом (его представителем) либо полученных из иных источников.

4) установление предполагаемой цели и характера деловых отношений;

5) иные меры в соответствии с Законом Республики Казахстан от 28 августа 2009 года № 191-IV «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансирования терроризма».

После проведения указанной выше надлежащей проверки Мерчанта,

3.1.2.4.2. платежные услуги оказываются на основании Договора-оферты, заключенного между Payment Processing и Мерчантом.

3.1.2.4.3. Договор-оферта является предложением для Мерчантов высылать свои оферты в адрес Payment Processing для заключения договора на условиях, определенных Договором-оферты и Заявки.

3.1.2.4.4. Направление оферты в адрес Payment Processing и акцепт оферты Payment Processing означают полное и безоговорочное принятие Мерчантом и Payment Processing всех условий Договора-оферты и Заявки без каких-либо изъятий и/или ограничений и равносителен заключению двухстороннего письменного Договора (ст. 394 ГК РК).

3.1.2.4.5. Порядок исполнения Договора-оферты регулируется исключительно нормами законодательства Республики Казахстан.

3.1.2.4.6. Мерчант направляет оферту для заключения Договора, после ознакомления с ним, путем заполнения Заявки, содержащей соответствующие действительности сведения, а также согласованную Сторонами в процессе предварительных переговоров Ставку вознаграждения, и направления сканированной (электронной) версии данной Заявки с подписью Мерчанта на электронный адрес Payment Processing: sales@ioka.kz или персональный адрес менеджера Payment Processing.

3.1.2.4.7. Payment Processing осуществляет акцепт оферты Мерчанта путем предоставления Мерчанту доступа к Системе. Payment Processing вправе отклонить оферту Мерчанта.

3.1.2.4.8. Мерчант обязуется сообщать при регистрации в Системе сведения, соответствующие действительности.

3.1.3. Порядок и сроки оказания услуги по приему платежей по карточкам

3.1.3.1. Покупатель взаимодействует с Payment Processing, осуществляя выбор необходимой ему услуги из перечня услуг, предоставляемых Интернет-магазином, с учетом Способа Платежа.

3.1.3.2. Для осуществления оплаты проводится Авторизация в зависимости от выбранного Покупателем Способа Платежа.

3.1.3.2.1. Авторизация может быть Одностадийной и Двустадийной:

- 1) Одностадийная Авторизация – Операция оплаты, при которой вся сумма платежа сразу списывается со счета Покупателя.
 - 2) 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 указанного счета Покупателя.

3.1.3.2.2. Мерчант по согласованию с Payment Processing выбирает наиболее удобный для себя вариант, если иное не устанавливается Payment Processing 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.

3.1.3.2.3. Перевод денег Мерчанту осуществляется после Обработки Операций Payment Processing в срок, не позднее 1 рабочего дня от даты обработки Payment Processing Авторизации операций. При этом Процессинг Двустадийной Авторизации проходит только после успешного завершения обеих стадий.

3.1.3.3. Порядок проведения Авторизации:

- 1) Покупатель в специальной электронной форме с использованием имеющегося у него компьютера/мобильного телефона/иного электронного устройства вводит реквизиты Платежной карточки, используемой для Операции оплаты.
- 2) По запросу Payment Processing Покупатель вводит дополнительные данные в зависимости от используемой технологии повышения безопасности платежей, в соответствии с правилами МПС.
- 3) Payment Processing осуществляет Авторизацию с предоставленными Покупателем реквизитами – в соответствии с Правилами МПС.
- 4) Payment Processing информирует Мерчанта о результате Авторизации – согласии с проведением Операции или отказе в проведении Операции.

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

3.1.3.5. Фиксация совершения указанных в п. 3.4.3 Порядка операций осуществляется Payment Processing в электронном виде и хранится в АПК Payment Processing. Выписки из АПК Payment Processing могут использоваться в качестве доказательств при рассмотрении споров, в том числе в судебном порядке.

3.1.3.6. Payment Processing 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, Payment Processing осуществляет Обработку Операций в отношении таких Авторизаций только после получения Payment Processing от Мерчанта запроса (так называемое «завершение авторизации»), подтверждающего необходимость Обработки Операции.

3.1.3.7. По результатам Обработки Операций Payment Processing направляет Мерчанту Отчет по успешно прошедшим транзакциям.

3.1.3.8. Payment Processing осуществляет расчеты с Мерчантом по всем Операциям, прошедшим Обработку Операций.

3.1.4. Порядок и сроки оказания услуги по выплате клиентам на карточки

3.1.4.1. Payment Processing в ежедневном круглосуточном режиме реального времени принимает от Мерчанта запросы на оказание услуг по выплате клиентам на Платежные карточки Visa, MasterCard (далее услуги «Процессинга»).

3.1.4.2. По факту получения такого запроса и при условии возможности оказания услуги Процессинга в соответствии Правилами МПС:

3.1.4.3. Payment Processing осуществляет списание денег с текущего счета Мерчанта в сумме проведения операции по Платежной карточке.

3.1.4.4. Payment Processing осуществляет обработку операций, обмен расчетными (клиринговыми) файлами с МПС и расчеты по таким операциям в сроки и в соответствии с Правилами МПС.

3.1.4.5. Payment Processing в режиме реального времени информирует Мерчанта о результате оказания услуги Процессинга в отношении каждой конкретной операции. При этом возможны следующие варианты:

- 1) Мерчант получил от Payment Processing сообщение с кодом ответа, указывающим на успешное совершение операции по Платежной карточке: услуга Процессинга в этом случае считается оказанной и подлежит оплате.

2) Мерчант получил от Payment Processing сообщение с кодом ответа, указывающим на не успешность совершение операции по Платежной карточке: услуга Процессинга в этом случае считается не оказанной и не подлежит оплате.

3) Мерчант не получил от Payment Processing сообщение с результатом совершения операции по Платежной карточке (к примеру, в результате коммуникационного сбоя и т.п.). В этом случае окончательный статус операции подлежит проверке и установлению в процессе проведения ежедневной сверки (в соответствии с далее описанным порядком). По итогам такой сверки Мерчант и Payment Processing устанавливают факт успешного проведения операции по Платежной карточке, и, если такой факт установлен, услуга Процессинга в этом случае считается успешно оказанной и подлежит оплате. В противном случае услуга Процессинга считается не оказанной и не подлежит оплате.

3.1.4.6. Payment Processing, в рабочие дни с 11:00 часов до 12:00 часов по времени г. Астаны, направляет Мерчанту Реестр, содержащий операции, в отношении которых оказаны услуги Процессинга за предыдущий рабочий и нерабочие/праздничные дни.

3.1.4.7. Payment Processing по рабочим дням по запросу Мерчанта, полученному в электронном виде, осуществляет в ручном режиме расследование и обработку операций в исключительных/нештатных ситуациях, возникших по ранее оказанным услугам Процессинга (в результате сбоев в работе систем, мошенничества, нештатных ситуаций), при условии, если Payment Processing обладает техническими возможностями такой обработки, и она допустима по Правилам МПС. Мерчант поручает Payment Processing списывать сумму денег с текущего счета или осуществлять зачисление денег на его текущий счет по результатам такого расследования и обработки операций. Payment Processing уведомляет Мерчанта в электронном виде о результатах такой обработки и произведенных расчетах.

4. Стоимость платежных услуг (тарифы)

Тарифы платежной организации ТОО «Payment Processing» по платежным услугам:

4.1. 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:

- Комиссии с каждой транзакции на прием платежей по Платежным карточкам Visa и Mastercard – 2.9%, минимальная комиссия – 30 тг.
- Комиссии с каждой транзакции на выплаты на Платежные карточки Visa и Mastercard – 3%, минимальная комиссия – 150 тг.

4.2. Payment Processing вправе предоставлять отдельным Мерчантам индивидуальные условия к утвержденным Тарифам.

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

5.1. Третья лица - это юридические лица и индивидуальные предприниматели, которые:

- предоставляют услуги платежной организации или действуют в интересах платежной организации, за исключением платёжных агентов и платёжных субагентов;
- не входят в группу компаний платежной организации и не являются работниками платежной организации.

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

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

5.4. 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.

5.5. Порядок взаимодействия при работе с поставщиками услуг.

1) Коммерческим отделом Платежной организации выявляется потребность физических лиц – резидентов РК по оплате сервисов Поставщиков услуг (в том числе, являющихся нерезидентами Республики Казахстан).

Ответственным сотрудникам коммерческого отдела проводятся маркетинговые исследования, включающие в себя анализ рынка, конкурентоспособности, потребительскую способность.

2) Также коммерческим отделом 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 Финансовым директором об установлении деловых отношений с Поставщиком услуг, определенный руководителем коммерческого отдела менеджер 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.

5.6. Заключение договора с Поставщиком услуг.

1) После осуществления действий, определенных п.5.5 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.
- 5.7. Технологическую возможность оказания Услуг Payment Processing обеспечивает самостоятельно и Банк. Payment Processing использует платежную платформу ioka, которая предоставляет комплексное решение для приема и совершения платежей <https://www.ioka.kz>. Банк оказывает услуги Процессинга.
- 5.8. Payment Processing информирует Банк о необходимости подключения нового Мерчанта, путем уведомления Банка.
- 5.9. Payment Processing обеспечивает подключение Мерчанта к Шлюзу и его дальнейшее использование, при условии надлежащего выполнения Мерчантом инструкций Payment Processing процедуры использования Шлюза, утвержденной Payment Processing, которая прилагается к Договору между Payment Processing и Мерчантом.
- 5.10. Payment Processing и Банк обязуются обеспечивать возможность непрерывного использования Шлюза и АПК Банка 24 часа в сутки и 7 дней в неделю, за исключением времени проведения плановых работ.
- 5.11. Банк обязуется письменно информировать Payment Processing о любых запланированных технических или других ожидаемых перерывах в работе Шлюза и АПК Банка не менее чем за 1 (один) рабочий день до принятия соответствующих мер.
- 5.12. Во время работы Шлюза должно быть обеспечено непрерывное соединение с АПК Банка.

Данные транзакций передаются в режиме реального времени из Шлюза в АПК Банка и наоборот в виде сообщения, сгенерированного в соответствии с форматом, указанным в технической документации Банка. Payment Processing передает данные в АПК Банка с обеспечением шифрования Данных транзакций в соответствии с требованиями Банка и с соблюдением стандартов PCI DSS в отношении безопасного хранения и передачи Данных транзакций.

6. Сведения о Системе управления рисками

- 6.1. Система управления рисками представляет собой систему организации, политик, процедур и методов, принятых Платежной организацией с целью своевременного выявления, измерения, контроля и мониторинга рисков Платежной организации для обеспечения её финансовой устойчивости и стабильного функционирования.
- 6.2. Платежная организация в целях эффективного управления рисками разработала политику управления рисками, которая состоит из систематической работы по разработке и практической реализации мер по предотвращению и минимизации рисков, выявлению, измерению, контролю и мониторингу рисков, оценки эффективности их применения, а также контролю за совершением всех денежных операций. В этих целях в Платежной организации закреплен работник (в случае отсутствия такого работника, данные функции выполняет Директор), выполняющий функции по управлению рисками, в задачи которого входит:

1. 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;
2. 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.

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

6.4. 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.

6.5. 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.

6.6. 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.

6.7. 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.

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

6.9. 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.

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

6.10.1. Мероприятия по управлению рисками:

1. определение организационной структуры управления рисками, обеспечивающей контроль за выполнением агентами и субагентами Платежной организации требований к управлению рисками, установленных правилами управления рисками Платежной организации;
2. определение функциональных обязанностей лиц, ответственных за управление рисками, либо соответствующих структурных подразделений;
3. доведение до органов управления Платежной организации соответствующей информации о рисках;
4. определение показателей бесперебойности функционирования Платежной организации;
5. определение порядка обеспечения бесперебойности функционирования Платежной организации;
6. определение методик анализа рисков;
7. определение порядка обмена информацией, необходимой для управления рисками;
8. определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев; определение порядка изменения операционных и технологических средств и процедур;
9. определение порядка оценки качества функционирования операционных и технологических средств, информационных систем;
10. определение порядка обеспечения защиты информации в Платежной организации.

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

Способы управления рисками:

1. установление предельных размеров (лимитов) обязательств агентов и субагентов Платежной организации с учетом уровня риска;
2. установление обеспечительного взноса агентов и субагентов Платежной организации в рамках оказываемых платежных услуг;
3. управление очередностью исполнения распоряжений должностными лицами;
4. осуществление расчета в платежной организации до конца рабочего дня;
5. осуществление расчета в пределах предоставленных агентами Платежной организации денежных средств;
6. обеспечение возможности предоставления лимита;
7. использование безотзывных банковских гарантий;
8. другие способы управления рисками.

7. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами

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

7.2. Плательщик 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: Республика Казахстан, почтовый индекс 050040, город Алматы, Бостандыкский район, улица Байзакова, дом 280;
- 2) путем личного обращения в офис платежной организации и ее наручным представлением по адресу: Казахстан, почтовый индекс 050040, город Алматы, Бостандыкский район, улица Байзакова, дом 280;

При каждом из перечисленных способов направления Платежной организации Претензии плательщика, 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 плательщика.

7.3. Обращения в службу технической поддержки плательщиков по телефону, направления сообщений через форму обратной связи на Сайте Системы 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, а также следующие документы:

- 1) копия документа, удостоверяющего личность плательщика;
- 2) документ, подтверждающий оплату (чек);
- 3) дополнительно может быть запрошена нотариально заверенная копия договора об оказании услуг сотовой связи, заключенного с оператором сотовой связи и предоставляющего плательщику право использования Абонентского номера, указанного плательщиком при регистрации Учетной записи Пользователя в Системе и др.

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

7.6. Для надлежащего рассмотрения претензии плательщика 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 плательщика дополнительно документы (или их копии), объяснения и иные сведения. По запросу Платежной организации плательщик обязан предоставить запрашиваемые Платежной организацией сведения и документы (их копии) в целях надлежащего досудебного урегулирования возникшего спора;

- проводит тщательный анализ полученных сведений и разъяснений для формирования полного и достоверного ответа на Претензию плательщика;
- подготавливает мотивированный письменный ответ плательщику на претензию.

7.7. Ответ на претензию плательщику подлежит направлению плательщику в срок, определенный п.7.5. Правил, по адресу, указаному в претензии, посредством службы доставки почтовых отправлений/корреспонденции.

7.8. 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.

7.9. 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 Payment Processing запрос на адрес электронной почты support@ioka.kz на обработку такой Операции: Поручение о возврате средств (если необходимо осуществить Операцию возврата) или гарантийное письмо (для других видов Операций) форма которой, устанавливается приложением к Договору между Payment Processing и Мерчантом.

7.10. К гарантийному письму Мерчант прилагает все имеющиеся у Мерчанта чеки, электронные записи и прочие документы, обосновывающие необходимость обработки такой Операции. Гарантийное письмо и Поручение о возврате денег должны быть подписаны лицами, имеющими право подписи, и скреплено оттиском печати Мерчанта.

7.11. 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.

7.12. Payment Processing рассматривает полученный от Мерчанта запрос и, при наличии возможности, осуществляет проведение запрошеннной Операции. Такая Операция в дальнейшем проходит Обработку операций аналогично всем прочим Операциям.

7.13. В случае выявления расхождения данных о принятых платежах Мерчанта и Итогового реестра платежей Payment Processing, обнаружившая расхождение Сторона направляет электронное письмо другой Стороне для проведения сверки и определения ошибки.

8. Порядок соблюдения мер информационной безопасности

8.1. 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.

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

- Гарантирование использования по назначению компьютеров и телекоммуникационных ресурсов Payment Processing ее сотрудниками, независимыми подрядчиками и другими пользователями.
- выявления, реагирования (противодействие атакам в реальном времени), разрешения и анализ причин возникновения инцидентов информационной безопасности.
- управления доступом к активам.
- антивирусной защиты.

- резервного копирования активов.
- управления непрерывностью бизнеса.
- регистрации, анализа и контроля событий информационной безопасности.
- выявление уязвимостей в информационных системах платежной организации, с использованием которых могут быть реализованы угрозы информационной безопасности.
- криптографической защиты, определения требований к организации работ, эксплуатации, обеспечению сохранности и безопасному использованию средств криптографической защиты.
- формирования принципов внесения изменений, процедуры установки, модификации и технического обслуживания информационных систем платежной организации.
- физической безопасности активов.
- защита сетевого периметра.
- соблюдение условий всех программных лицензий, авторских прав и законов, касающихся интеллектуальной собственности.

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

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

8.2. Система информационной безопасности платежной организации

8.2.1. Система информационной безопасности, являющаяся совокупностью применяемых в платежной организации мер по защите информации, создаётся в соответствии с методологией менеджмента информационной безопасности, описанной в политике информационной безопасности платежной организации, и состоит из следующих элементов. Средства и меры предотвращения несанкционированного доступа к программно-техническим средствам, применяемые в Платежной организации, включая программно-технические средства защиты, должны обеспечивать уровень защиты информации и сохранение ее конфиденциальности в соответствии с требованиями, установленными законодательством Республики Казахстан. Все сотрудники обязуются принимать все необходимые меры по сохранению конфиденциальности, предотвращению несанкционированного использования и защите идентификационных данных от несанкционированного доступа со стороны третьих лиц.

8.3. Обеспечение безопасности вычислительных сетей.

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

8.3.2. Сервер

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

8.3.3. Рабочие станции

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

8.4. Управление доступом пользователей к данным

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

8.5. Управление учётными записями и парольной защиты

8.5.1. Работа пользователей в ОС и ИС осуществляется под уникальными учётными записями. Не допускается работа пользователя под чужой учетной записью и учетной записью «Администратор», а также включение пользователя в привилегированную группу «Администраторы». Учетная запись «Гость» в операционной системе должна быть отключена. Аутентификация на сервере осуществляется путём подключения к терминалу и ввода пользователем персональных данных созданных Системным администратором. Для предоставления временного доступа к ресурсам Payment Processing (для лиц, не являющихся работниками Payment Processing, для работников, которым необходимо получить временный доступ к ресурсам Payment Processing и т.п.) необходимо использовать временные учетные записи (с фиксированным сроком действия) в ОС.

8.5.2. Пароли учетных записей в ОС и ИС. Пароли оборудования

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

символов (имена, фамилии, наименование автоматизированного рабочего места - АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.).

8.5.3. Встроенные учетные записи

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

8.5.4. При увольнении работника

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

8.6. Обеспечение антивирусной защиты

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

8.6.2. Сервер

8.6.2.1. Сервер должен обязательно иметь установленное антивирусное программное обеспечение для автоматической проверки всех файлов и электронной почты,

поступающих на этот сервер. Не реже 1 раза в неделю на терминальном сервере с установленной ОС должно проводиться полное сканирование всех дисков компьютера на предмет заражения вирусами. Антивирусное программное обеспечение на сервере должно обновляться не реже одного раза в день, автоматически путем соответствующих настроек антивирусного ПО.

8.6.3. Рабочие станции

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

8.7. Обеспечение физической безопасности

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

8.8. Обеспечение безопасной поддержки и эксплуатации информационной инфраструктуры

8.8.1. Для обеспечения максимальной прозрачности и безопасности разработки, внедрения и эксплуатации компонентов информационной инфраструктуры платежной организации, а также их программного обеспечения изменения, вносимые в информационную инфраструктуру, подлежат тестированию и регистрации. Требования информационной безопасности учитываются при разработке, внедрении и эксплуатации информационных систем, отдельных компонентов и программного обеспечения.

8.9. Мониторинг информационной инфраструктуры

8.9.1. Мониторинг информационной инфраструктуры необходим для своевременного выявления инцидентов и уязвимостей информационной безопасности. Мониторинг осуществляется в отношении производительности систем, доступа к данным, функционирования систем безопасности. Для оценки общего уровня защищенности информационной инфраструктуры платежной организации выполняются проверки на уязвимости. Независимый аудит системы безопасности и внутренних контролей проводится на регулярной основе не реже одного раза в год.

8.10. Управление инцидентами и уязвимостями информационной безопасности

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

8.11. Обеспечение бесперебойной работы информационной инфраструктуры

8.11.1. Поскольку одной из задач ИБ является обеспечение доступности информации, мерам по защите компонентов информационной инфраструктуры от сбоев отводится значительная роль. Для обеспечения отказоустойчивости применяется дублирование критичных компонентов информационной инфраструктуры. Средствами резервного копирования обеспечивается гарантированное восстановление бизнес-процессов после сбоя в работе одного или нескольких компонентов информационной инфраструктуры, а также обеспечивается минимизация времени восстановления сервисов и бизнес-процессов. Платежная организация обеспечивает бесперебойное функционирование Системы в режиме 24/7/365 (24 часа в день, 7 дней в неделю, 365 дней в году), за исключением времени проведения профилактических работ.

8.12. Организация и ответственность

8.12.1. Руководство платежной организации регулирует вопросы, связанные с:

8.12.1.1. определением целей и стратегии достижения целей обеспечения информационной безопасности в платежной организации;

8.12.1.2. выделением ресурсов для осуществления деятельности по обеспечению информационной безопасности в платежной организации;

8.12.1.3. принятием решений в отношении ключевых рисков нарушения информационной безопасности.

8.12.2. Менеджер Департамента ИТ несёт ответственность за:

8.12.2.1. определение требований по информационной безопасности и осуществление контроля исполнения данных требований в платежной организации;

8.12.2.2. осуществление контроля общей эффективности обеспечения информационной безопасности, её соответствия текущим и будущим требованиям бизнеса.

8.12.3. Владельцы процессов и активов несут ответственность за:

8.12.3.1. распределение полномочий и ответственности по реализации мер обеспечения информационной безопасности (конфиденциальности, целостности, доступности) для своих активов, адекватных существующим рискам;

8.12.3.2. устранение в установленные сроки несоответствий по результатам проведенных аудитов/проверок обеспечения ИБ.

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

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

