УТВЕРЖДЕНЫ
Решением №2 единственного участника
ТОО «Байсанақ жиын»
от 31 мая 2024 года

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ ТОО «OnePay LTD»

Алматы 2024 год

ОГЛАВЛЕНИЕ

Общие положения (Термины и определения)

Настоящие правила осуществления деятельности **Товарищества с ограниченной ответственностью «OnePay LTD»** в качестве платежной организации (далее – «Правила» и «Платежная организация» соответственно) разработаны в соответствии с Законом Республики Казахстан «О платежах и платежных системах» (далее – Закон о платежах), Постановлением Правления Национального банка Республики Казахстан № 215 от 31 августа 2016 года «Об утверждении Правил организации деятельности платежных организаций», и определяют порядок организации деятельности платежной организации, включающий оказание платежных услуг платежной организацией, взаимодействие платежной организации с третьими лицами, в том числе с физическими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией, а также процедуры урегулирования спорных ситуаций и разрешения споров с клиентами при оказании платежных услуг.

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

- **Банк-эквайер** – банк, обеспечивающий проведение операций по платежным картам.
- **Бенефициарный собственник** – физическое лицо:
  - которому прямо или косвенно принадлежат более 25 процентов долей участия в уставном капитале либо размещенных (за вычетом привилегированных и выкупленных обществом) акций клиента - юридического лица или иностранной структуры без образования юридического лица;
  - осуществляющее контроль над Клиентом иным образом;
  - в интересах которого Клиентом совершаются операции с деньгами и (или) иным имуществом;
- **Бесперебойность функционирования платежной организации** – комплексное свойство платежной организации «OnePay LTD», обозначающее ее способность предупреждать нарушения надлежащего функционирования (в том числе не допускать приостановления (прекращения) осуществления операций или ненадлежащего осуществления операций), а также восстанавливать надлежащее функционирование в случае его нарушения.
- **Инцидент информационной безопасности** – отдельно или серийно возникающие сбои в работе информационно-коммуникационной инфраструктуры или отдельных ее объектов, создающие угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов платежной организации.
- **Клиент/Плательщик** – физическое лицо, обладающее надлежащей дееспособностью в соответствии с законодательством Республики Казахстан для осуществления платежа, совершившее конклюдентные действия, направленные на заключение с Платежной организацией договора об оказании услуг.
- **Международные платежные системы (МПС)** – международные платежные системы: Visa International и MasterCard International и иные МПС.
- **Оферта** – публичная оферта на предоставление платежных услуг Платежной организацией физическим лицам, являющийся договором присоединения согласно положениям статьи 389 и 395 Гражданского кодекса Республики Казахстан, размещенный на сайте Платежной организации.
- **Оценка риска** – оценка вероятности реализации риска и величины возможных потерь при реализации конкретного вида риска и/или совокупных рисков (группы рисков), принимаемых на себя платежной организацией.

- **Платежная организация – Товарищество с ограниченной ответственностью «OnePay LTD»** (БИН 240540027226), созданное и действующее в соответствии с законодательством Республики Казахстан.
- **Платежная услуга** – услуга, оказываемая платежной организацией Клиенту в соответствии с Законом Республики Казахстан «О платежах и платежных системах».
- **Поставщик услуг/Партнер** – юридическое лицо или физическое лицо, зарегистрированное в качестве индивидуального предпринимателя, заключившее отдельный договор с платежной организацией, и в пользу которого Клиент осуществляет платеж в счет оплаты за Товары, либо физическое лицо, принимающее денежные средства от Клиента, не связанные с предпринимательской деятельностью.
- **Расчетный банк/Банк** – банк второго уровня, с которым платежная организация заключила договоры в целях оказания платежных услуг.
- **Риск** – присущая деятельности платежной организации возможность (вероятность) возникновения убытков, ухудшения ликвидности или иных негативных последствий вследствие наступления неблагоприятных событий, связанных с внутренними факторами (сложность организационной структуры, уровень квалификации работников, организационные изменения, текучесть кадров и т.д.) и внешними факторами (изменение экономической конъюнктуры, применяемые новые технологии, внедрение новых продуктов и т.д.).
- **Система по учету платежей (Система)** – совокупность программно-технических средств платежной организации, обеспечивающих информационно-технологическое взаимодействие, регистрацию и осуществление платежей и иных операций в соответствии с настоящими правилами.
- **Специальный счет (Транзитный счет)** – внутренний (транзитный) счет, открытый в Банке для Платежной организации по договору.
- **Товар** – товары, работы, услуги, права на результаты интеллектуальной деятельности, реализуемые поставщиком услуг конечным потребителям (клиентам) для личного, семейного или домашнего использования.
- **Транзакция** – финансовая операция с картой, либо электронными деньгами в результате которой производится оплата каких-либо товаров или услуг, или перевод.
- **Третьи лица** – юридические лица и физические лица – индивидуальные предприниматели, которые предоставляют технологическое обеспечение платежных услуг или иным образом действуют в интересах платежной организации, и не являются аффилированными с платежной организацией.
- **Шлюз** – программное обеспечение для создания электронного канала, посредством которого производится обмен данными по транзакциям и данными.

1. Описание платежных услуг, оказываемых Платежной организацией.

1.1. 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 осуществляются Платежной организацией на основании отдельных договоров, заключенных с банком/ банками второго уровня и платежной организацией с Партнерами и обеспечивает прием платежей инициированных с использованием платежных карт с указанием реквизитов назначения соответствующего платежа и бенефициара соответствующего платежа с последующим обеспечением передачи реквизитов по платежу для

его исполнения в адрес соответствующего банка, а банк в свою очередь исполняет указание Клиента, переданное через Систему Платежной организации в электронной форме.

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

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

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

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

- Клиент посредством сети интернет/ мобильного телефона заходит в соответствующее приложение/сайт Поставщика услуг;
- Клиент знакомится с условиями предоставления платежной услуги и соглашается с условиями Оферты на платежной странице;
- Клиент в приложении/сайте инициирует платеж в пользу Поставщика услуг;
- Клиент вводит персональные данные в приложении/сайте Поставщика услуг
- Для оплаты платежа Клиент вводит реквизиты банковской карты;
- Платежная организация посредством запроса в Банк инициирует распоряжение Клиента, полученного в электронной форме;
- Банк-эквайер, получив подтверждение от Платежной организации и Клиента производит списание с банковской карты Клиента, и перевода Платежа в пользу Поставщика услуг, указанного в поручении Клиента, сумму инициируемой Клиентом операции с учетом вознаграждения Платежной организации или перевод платежа со счета банка – эквайера на специальный счет Расчетного банка, с которым у Платежной организации заключен соответствующий договор.
- После зачисления платежей на специальный счет Платежная организация передает в электронном виде Расчетному банку поручение с указанием суммы и реквизитов Поставщика услуг, которому необходимо зачислить платежи, после чего Расчетный банк осуществляет перевод платежей на расчётный счет Поставщика услуг.

- Платежная организация получает от Банка подтверждение исполнения операции;
- Платежная организация выдает Клиенту электронную квитанцию, подтверждающую совершение Клиентом операции.

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

Сроки оказания платежной услуги – от 1 (одного) до 3 (трех) рабочих дней, следующего за днем приема платежа.

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

Тарифы платежной организации ТОО «OnePay LTD» по платежным услугам:

3.1. Услуги Платежной организации 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 при осуществлении деятельности по интернет эквайрингу составляют от 0 до 10 % от суммы операции, в зависимости от категории сервисов, которые взимаются с Клиента:

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

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

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

- проводятся маркетинговые исследования, включающие в себя анализ рынка, конкурентоспособности, потребительскую способность;
- финансовой службой проводится экономическое обоснование заведения нового Поставщика услуг в систему Платежной организации, а также выявляется платежная нагрузка на Клиентов;
- после проведения вышеуказанных действий и принятия положительного решения по работе с Поставщиком услуг, у последнего запрашиваются все необходимые документы в рамках ПОД/ФТ и проводится полный анализ комплаенс рисков.
- в случае отсутствия комплаенс рисков производится обмен технической документацией для подключения Поставщика услуг к системе Платежной организации по протоколу технического взаимодействия API.

4.1.1. Заключение договора с Поставщиком услуг.

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

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

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

– Платежная организация обязана передавать Поставщику услуг данные о каждом принятом платеже для внесения изменений в лицевой счет клиента. Сведения должны быть переданы непосредственно в период приема платежа на основании данных, указываемых клиентом, без ошибок и искажений.

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

– В соответствии с требованиями бизнесов и рисков, связанных с утечкой и разглашением конфиденциальной информации, к которой осуществляется доступ третьей стороной, работниками отдела информационных технологий по согласованию с третьей стороной осуществляется контроль должного уровня обслуживания и уровня информационной безопасности третьей стороны. Контроль может включать: - анализ отчетов о работах (услугах), предоставляемых третьей стороной; - регулярные совещания по вопросам и проблемам, возникающим в ходе работ; - анализ отчетов и результатов расследования возникших инцидентов ИБ; - актуальность сертификатов по информационной безопасности (если применимо).

4.2. Порядок взаимодействия Платежной организации с Банками.

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

Платежная организация проходит регистрацию в Системе Банка, для чего:

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

– Стороны проводят техническое тестирование систем;

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

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

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

– Сведения должны быть переданы непосредственно в период обработки платежа;

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

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

– На ежемесячной основе производится сверка взаиморасчетов.

Детализированное описание передвижения денежных средств при положительно обработанной операции оплаты:

– Банк-эмитент осуществляет списание денег с Карты Плательщика;

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

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

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

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

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

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

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

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

5. Сведения о системе управления рисками, используемой Платежной организацией

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

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

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

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

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

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

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

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

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

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

В основу управления рисками положены следующие принципы:

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

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

Мероприятия по управлению рисками:

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

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

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

4) определение показателей бесперебойности функционирования платежной организации;

5) определение порядка обеспечения бесперебойности функционирования платежной организации;

6) определение методик анализа рисков;

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

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

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

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

11) определение порядка обеспечения защиты информации в платежной организации.

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

Способы управления рисками:

1) управление очередностью исполнения распоряжений должностными лицами;

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

3) обеспечение возможности предоставления лимита;

4) установление предельных размеров (лимитов) обязательств контрагентов Платежной организации с учетом уровня риска;

5) осуществление расчета в пределах, предоставленных агентами Платежной организации денежных средств;

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

7) другие способы управления рисками.

6. Порядок урегулирования спорных ситуаций и разрешения споров с Клиентами

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

Клиент обязан обратиться к платежной организации с письменным заявлением, составленным в произвольной форме, содержащим указание на возникшую спорную ситуацию (далее – «Претензия») путем направления его почтовым отправлением по адресу - Республика Казахстан, город Алматы, Розыбакиева 37.

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

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

Ко всем Претензиям, направляемым Клиентами Платежной организации, должны быть приложены надлежащим образом оформленные копии документов, подтверждающие факты, указанные в Претензии, а также следующие документы:

1. копия документа, удостоверяющего личность клиента, в случае отсутствия интеграции с объектами информатизации государственных органов и (или) государственных юридических

лиц, невозможности идентификации субъекта с использованием технологических средств, а также в иных случаях, предусмотренных законами Республики Казахстан.

2. документ, подтверждающий оплату (чек).

3. дополнительно может быть запрошена нотариально заверенная копия договора об оказании услуг сотовой связи, заключенного с оператором сотовой связи и предоставляющего клиенту право использования абонентского номера, указанного клиентом при регистрации учетной записи клиента в системе и др.

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

1. Для надлежащего рассмотрения Претензии Клиента и подготовки ответа платежная организация:

2. привлекает к всестороннему изучению спора сотрудников компетентных подразделений (технических, правовых, расчетных, и иных структурных подразделений для получения разъяснений, дополнительных сведений и иных данных в отношении оспариваемой ситуации);

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

4. проводит тщательный анализ полученных сведений и разъяснений для формирования полного и достоверного ответа на Претензию клиента;

5. подготавливает мотивированный письменный ответ клиенту на Претензию.

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

7. Порядок соблюдения мер информационной безопасности

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

Методами обеспечения защиты информации в платежной организации являются:

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

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

Идентификация пользователей, персонала и ресурсов информационной системы.

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

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

Регистрация (протоколирование) обращений к защищаемым объектам и информации.

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

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

Защита информационной системы платежной организации осуществляется с целью исключения возможностей:

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

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

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

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

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

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

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

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

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

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

7.5. Требования по организации хранения и использования паролей:

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

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

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

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

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

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

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

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

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

7.6. Запрещается:

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

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

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

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

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

информационных рисков выбираются соответствующие меры по их обработке и дальнейшему совершенствованию.

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

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

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

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

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

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

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

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

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

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

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

- порядок проведения анализа причин инцидента информационной безопасности ответственным сотрудником (должностным лицом, ответственным за обеспечение информационной безопасности) совместно с соответствующими подразделениями после принятия мер по выявленным инцидентам;
- предупреждение причин инцидентов информационной безопасности и разработка мер по предотвращению возникновения таких ситуаций или снижению возможности причинения вреда в случае их возникновения (в том числе с привлечением ответственного сотрудника);
- изучение соответствующих отчетов программно-технических средств и получение объяснений от сотрудников, вызвавших инцидент информационной безопасности (внутренние инциденты);
- классификация нежелательных явлений по степени негативного воздействия и их оценка на основе критериев оценки.

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

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

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

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

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

8.1. Программно-технические средства, используемые платежной организацией при оказании Платежных услуг, включают в себя:

8.1.1. систему интернет-эквайринга, представляющую собой совокупность программно-технических средств, документации и организационно-технических мероприятий, позволяющих осуществлять операции, связанные с платежами;

8.1.2. оборудование – физические серверы и сетевое оборудование, размещаемые в дата-центрах поставщиков услуг, обслуживание которых осуществляется специалистами поставщиков услуг и платежной организации.

8.2. Система интернет-эквайринга.

8.2.1. Цель использования системы интернет-эквайринга заключается в обеспечении взаимодействия между ее участниками, включающими интернет-магазины, клиентов и платежные сервисы, в соответствии с едиными стандартами вне зависимости от того, с использованием какого платежного сервиса осуществляется оплата соответствующего Товара.

8.2.2. Система интернет-эквайринга функционирует на основании электронных счетов, формируемых поставщиками услуг по запросу клиента. Запрос на выставление электронного счета создается либо полностью в автоматическом режиме (через API), либо в ручном режиме через доступный поставщику услуги web-интерфейс. Поставщики услуг получают информацию о поступлении платежа сразу же после оплаты в режиме реального времени.

8.2.3. Подключение платежных сервисов реализуется путем их подключения к электронному шлюзу системы интернет-эквайринга, предоставляющему возможность взаимодействия с различными типами международных платежных сервисов, включая:

8.2.3.1. интернет-эквайринг банковских карт;

8.2.3.2. системы мобильных платежей.

8.2.4. Контроль функционирования системы интернет-эквайринга обеспечивает автоматизированный онлайн бэк-офис, позволяющий оперативно подключать к системе новых поставщиков услуг, проводить операции и сверки в режиме реального времени, а также устанавливать и корректировать настройки безопасности в зависимости от типа той или иной операции или запроса участника системы интернет-эквайринга.

8.2.5. Функционал системы интернет-эквайринга включает в себя следующие уникальные модули:

8.2.5.1. шлюзы для подключения платежных сервисов;
8.2.5.2. автоматическое подключение к системе;
8.2.5.3. система выставления и учета электронных счетов;
8.2.5.4. система управления платежным шлюзом;
8.2.5.5. API для подключения интернет-магазинов;
8.2.5.6. модули для подключения к CMS;
8.2.5.7. подключение к системам бронирования;
8.2.5.8. клиентский интерфейс магазинов;
8.2.5.9. формирование юридических и бухгалтерских документов;
8.2.5.10. интеграция с биллингом и системой контроля доступа;
8.2.5.11. сервис возврата, отмены и корректировки ошибочных платежей;
8.2.5.12. сервис произвольных выплат;
8.2.5.13. модуль информирования плательщиков;
8.2.5.14. сервис выставления ручных счетов;
8.2.5.15. фильтры для противодействия мошенничеству через систему (фильтры антифрод);
8.2.5.16. статистическая отчетность;
8.2.5.17. модуль сверки реестров.

8.2.6. Использование системы интернет-эквайринга позволяет оперативно и технически безопасно объединять несколько платежных сервисов и предоставлять к ним доступ для интернет-магазинов через единый интерфейс в рамках одной технической интеграции. Система интернет-эквайринга также объединяет и сами интернет-магазины, предоставляя клиентам возможность выбирать различные товары на одном интернет-сайте и осуществлять оплату единым платежом, подключая любые платежные сервисы (в том числе, производить доплату по

тому или иному заказу с другого платежного сервиса в случае, если на первоначально выбранном платежном сервисе недостаточно средств для оплаты).

9. Порядок внесения изменений в настоящие Правила

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

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

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

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

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

Пронумеровано и прошнуровано

на 17 (семнадцати)

страницах

Подпись