

УТВЕРЖДЕНЫ:

Приказом Директора ТОО «Airba Pay»

№ 6 от «17» июня 2024 г.



А.С. Барышков

**Правила
осуществления деятельности платежной организации
Товарищества с ограниченной ответственностью «Airba Pay»**

Алматы
2024 год

СОДЕРЖАНИЕ

1. Основные положения	3
2. Термины и определения	3
3. Описание платежных услуг, оказываемых Платежной организацией	5
4. Порядок и сроки оказания платежных услуг Клиентам Платежной организации	5
5. Стоимость платежных услуг (тарифы), оказываемых Платежной организацией	7
6. Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых Платежной организацией	8
7. Сведения о Системе управления рисками, используемой Платежной организацией	9
8. Порядок урегулирования спорных ситуаций и разрешения споров с Клиентами	10
9. Порядок соблюдения мер Информационной безопасности	10
10. Описание программно-технических средств и оборудования, необходимого для оказания платежных услуг	13
11. Порядок внесения изменений в Правила	15

1. Основные положения

1.1. Настоящие Правила осуществления деятельности платежной организации Товарищества с ограниченной ответственностью «Airba Pay» (далее - Правила) разработаны в соответствии с Законом Республики Казахстан от «26» июля 2016 года «О платежах и платежных системах» (далее – Закон о платежах), Постановлением Правления Национального Банка Республики Казахстан от «31» августа 2016 года № 215 «Об утверждении Правил организации деятельности платежных организаций» и другими нормативно-правовыми актами Республики Казахстан, а также внутренними документами Товарищества с ограниченной ответственностью «Airba Pay» (далее – AIRBA PAY или Платежная организация).

1.2. Правила определяют единые условия и процедуры, обеспечивающие осуществление операций в системе AIRBA PAY и устанавливают общие требования к порядку оказания Услуг по обработке платежей, инициированных Клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам.

1.3. Настоящие Правила обязательны для исполнения всеми Участниками платежа. Каждый из Участников гарантирует другим Участникам, что обладает необходимой правоспособностью (правосубъектностью), а равно всеми правами и полномочиями, необходимыми и достаточными для присоединения к настоящим Правилам и исполнения обязательств в соответствии со всеми их условиями.

1.4. Заключение физическими лицами в рамках Платежной организации договоров осуществляется в соответствии с Гражданским кодексом Республики Казахстан. При этом, Договор считается заключенным и вступает в силу с момента совершения физическим лицом действий, предусмотренных в Публичной оферте на оказание ТОО «Airba Pay» физическим лицам платежных и информационно-технологических услуг, направленных на обеспечение взаимодействия при совершении оплаты, перевода и (или) получения выплаты в системе «airbapay.kz» (далее – Договор), размещенной на сайте по адресу: <https://ecom.airbapay.kz/>.

2. Термины и определения

2.1. Применяемые в тексте настоящих Правил, термины имеют следующее значение:

Бесперебойность функционирования Платежной организации – комплексное свойство Платежной организации, 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.

Информационная безопасность – состояние защищенности электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Информационно-коммуникационная инфраструктура (Информационная инфраструктура) – совокупность объектов информационно-коммуникационной инфраструктуры, предназначенных для обеспечения функционирования технологической среды в целях формирования электронных информационных ресурсов и предоставления доступа к ним.

Информационный актив – совокупность информации и объекта Информационно-коммуникационной инфраструктуры, используемого для ее хранения и/или обработки.

Информация об инцидентах информационной безопасности – информация об отдельно или серийно возникающих сбоях в работе Информационно-коммуникационной инфраструктуры или

отдельных ее объектов, создающих угрозу их надлежащему функционированию и (или) условия для незаконного получения, копирования, распространения, модификации, уничтожения или блокирования электронных информационных ресурсов Платежной организации.

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.

Обеспечение информационной безопасности – процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов Платежной организации.

Партнер – юридическое лицо, индивидуальный предприниматель, частный нотариус, адвокат, частный судебный исполнитель, принимающий платежи Платежной организации для оплаты за поставляемые ими товары, работы и услуги.

Периметр защиты информационно-коммуникационной инфраструктуры – совокупность программно-аппаратных средств, отделяющих Информационно-коммуникационную инфраструктуру Платежной организации от внешних информационных сетей и обеспечивающих защиту от угроз Информационной безопасности.

Платеж - исполнение денежного обязательства с использованием наличных денег и (или) платежных инструментов.

Клиент/Плательщик – физическое лицо (обладающее надлежащей дееспособностью) или юридическое лицо, получающие платежную услугу.

Получатель платежа – 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.

Система AIRBA PAY (Система) – совокупность программно-технических средств, документации и организационно-технических мероприятий, обеспечивающих осуществление платежей.

Угроза информационной безопасности – совокупность условий и факторов, создающих предпосылки к возникновению Инцидента информационной безопасности.

Участники платежа и (или) перевода денег - физические и юридические лица, филиалы и представительства юридических лиц, имеющие права и (или) обязанности по платежу и (или) переводу денег.

Электронное сообщение – любое сообщение, составленное электронным способом и передаваемое между Участниками платежа, по защищенному каналу связи.

Message-подтверждение платежей - способ удостоверения распоряжения Клиента о совершении платежа посредством отправки сообщения с использованием программы-мессенджера для абонентского устройства Клиента под управлением мобильных операционных систем с целью удаленного доступа Клиента к Системе.

Система управления рисками - система организации политик процедур и методов, принятых Платежной организацией, позволяющих своевременно осуществлять выявление, изменение, контроль, мониторинг за возникающими рисками, а так-же разработку мероприятий по

минимизации рисков при оказании платежных услуг.

3. Описание платежных услуг, оказываемых Платежной организацией

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.

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 осуществляется путем взаимодействия Системы с программно-аппаратными комплексами банков и (или) организаций, осуществляющих отдельные виды банковских операций, совершаемого с соблюдением требований действующего законодательства Республики Казахстан.

4. Порядок и сроки оказания платежных услуг Клиентам Платежной организации

4.1. 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 (далее – «обслуживающий банк», «платежная услуга») осуществляется следующим образом:

1) Платежная организация, в рамках договора, заключенного с обслуживающим банком, обеспечивает обработку платежей инициированных с использованием банковских карт с указанием реквизитов назначения соответствующего платежа и бенефициара соответствующего платежа с последующим обеспечением передачи реквизитов по платежу для его исполнения в пользу соответствующего обслуживающего банка, а последний в свою очередь исполняет указание Клиента, переданное через Платежную организацию 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 банковской карты Клиента, с их зачислением в пользу обслуживающего банка с целью последующего исполнения поручения/ распоряжения Клиента полученного Платежной организацией от Клиента и переданного Платежной организацией в обслуживающий банк.

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

- Клиент посредством сети интернет/ мобильного телефона, терминала самообслуживания заходит в соответствующее приложение Платежной организации или на WEB-страницу/приложение Парнера/поставщика услуг и подтверждает покупку товара/услуги;

- Клиент знакомится с тарифом/ размером комиссии за предоставление Платежной

организацией соответствующей услуги;

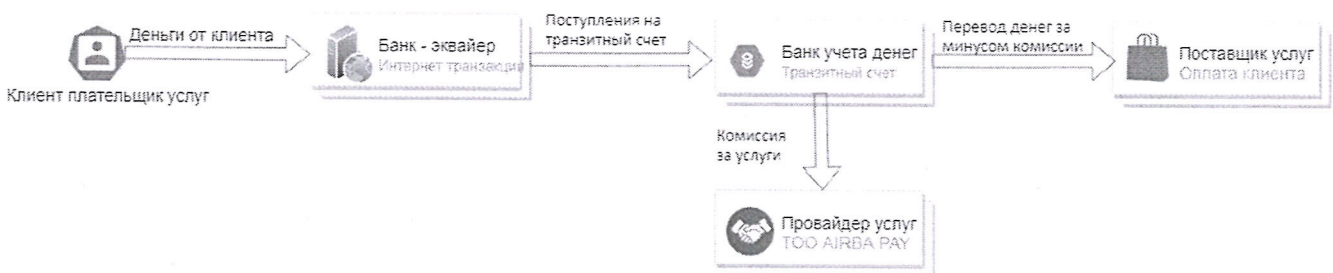
- Клиент знакомится с условиями предоставления платежной услуги и соглашается с условиями Договора;
- Клиент в приложении или на WEB-странице инициирует платеж в пользу Партнера/поставщика услуг;
- Клиент вводит в электронное приложение реквизиты для исполнения платежа обслуживающим банком;
- Для оплаты платежа Клиент вводит реквизиты банковской карты, банковского счета;
- Платежная организация посредством запроса в обслуживающий банк инициирует распоряжение Клиента, полученного в электронной форме;
- Обслуживающий банк, получив подтверждение от Платежной организации и Клиента, производит списание с банковской карты суммы инициируемой Клиентом операции с учетом комиссионного вознаграждения Платежной организации;
- Платежная организация получает от обслуживающего банка подтверждение исполнения операции;
- Платежная организация выдает Клиенту электронное подтверждение, подтверждающее совершение Клиентом операции и списание с Клиента комиссии Платежной организации;
- Обслуживающий банк на основании данных, полученных в электронной форме во время транзакции, производит перевод денег по транзакциям через транзитный счет Платежной организации на текущий счет Партнера/поставщика услуг, за вычетом комиссионного вознаграждения обслуживающего банка и Платежной организации;
- Перевод обслуживающим банком на текущий счет Партнера/поставщика услуг по совершенным транзакциям производится обслуживающим банком в национальной валюте Республики Казахстан.

Сроки оказания платежной услуги - в течение 1 (одного) – 4 (четырех) рабочих дней со дня, следующего за днем приема платежа.

Допустимый срок хранения данных держателей карт составляет 5 (пять) лет.



Структура движения денег по POS транзакциям в пользу поставщика



Структура движения денег по карточным транзакциям в пользу поставщика

5. Стоимость платежных услуг (тарифы), оказываемых Платежной организацией

Тарифы Платежной организации по платежным услугам:

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:

№	Наименование категорий сервисов, предоставляемых Партнерами/поставщиками услуг	Дополнительная плата (допустимая дополнительная комиссия) взимаемая с Клиента
1.	Игровые сервисы	от 0 % до 5% от суммы операции
2.	Букмекеры	от 0 % до 15% от суммы операции
3.	Социальные сети	от 0 % до 5% от суммы операции
4.	Сотовые операторы	от 0 % до 5% от суммы операции
5.	Подарочные карты, купоны	от 0 % до 5% от суммы операции
6.	ЖКХ	от 0 % до 5% от суммы операции
7.	MLM	от 0 % до 5% от суммы операции
8.	Интернет и телефония	от 0 % до 5% от суммы операции
9.	Хостинг	от 0 % до 5% от суммы операции
10.	Благотворительность	Не взимается
11.	Реклама	от 0 % до 5% от суммы операции
12.	Страхование	от 0 % до 5% от суммы операции
13.	Интернет – магазины, розничные магазины (офлайн)	от 0 % до 5% от суммы операции
14.	Билеты (авиа, ж/д)	от 0 % до 5% от суммы операции
15.	МФО, ломбарды, прочие финансовые организации	от 0 % до 10% от суммы операции
16.	Прочие виды сервисов, не включенные в отдельные категории	от 0 % до 5% от суммы операции

- Стоимость дополнительной платы (допустимой дополнительной комиссии (верхняя комиссия) взимаемой с Клиента устанавливается в соответствии с договорными условиями, указанными в договорах, заключенных между AIRBA PAY и Партнерами/поставщиками услуг.

- Ценовая политика по взимаемой дополнительной комиссии с Плательщика устанавливается Платежной организацией самостоятельно в рамках допустимых значений,

указываемых в договорах.

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

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

6. Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых Платежной организацией

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

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

Подключение информационных систем третьей стороны к системам Платежной организации производится на основании заключенного договора на оказание информационных и/или технологических услуг или договоров поручения на прием платежей, которые обязательно включают в себя пункты о неразглашении конфиденциальной информации.

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

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

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

6.2. Порядок взаимодействия при работе с Партнерами/поставщиками услуг включает в себя следующие мероприятия:

- Проводятся маркетинговые исследования, включающие в себя анализ рынка, конкурентоспособность, потребительскую способность.

- Финансовой службой проводится экономическое обоснование заведения нового Партнера/поставщика услуг в систему Платежной организации, а также выявляется платежная нагрузка на Клиентов.

- После проведения вышеуказанных действий и принятия положительного решения по работе с Партнером/поставщиком услуг, у последнего запрашиваются все необходимые документы в рамках соблюдения законодательства Республики Казахстан в области противодействия легализации (отмыванию) доходов, полученных преступным путем, и

финансированию терроризма, и проводится полный анализ комплаенс рисков.

- В случае отсутствия комплаенс рисков производится обмен технической документацией для подключения Партнера/поставщика услуг к системе Платежной организации по протоколу технического взаимодействия API.

7. Сведения о Системе управления рисками, используемые Платежной организацией

7.1. Платежная организация с целью эффективного управления рисками разработала и утвердила Систему управления рисками ТОО «AIRBA PAY», которая состоит из следующих блоков:

- управление рисками;
- анализ и управление финансовыми рисками;
- правовой риск;
- риск информационной безопасности.

7.2. Система управления рисками Платежной организации состоит из систематической работы по разработке и практической реализации мер по предотвращению и минимализации 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.

7.3. 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.

7.4. Процесс управления рисками в Платежной организации включает в себя:

- Анализ и оценка риска, включающий в себя систематическое определение:
 1. объектов анализа риска;
 2. индикаторов риска по объектам анализа риска, определяющих необходимость принятия мер по предотвращению и минимизации рисков;
 3. оценка возможного ущерба в случае возникновения рисков.
- Разработка и реализация практических мер по управлению рисками с учетом:
 1. вероятности возникновения рисков и возможных последствий;
 2. анализа применения возможных мер по предотвращению и минимизации рисков.

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

- Размер, характер и сложность бизнеса;
- Доступность рыночных данных для использования в качестве исходной информации;
- Состояние информационных систем и их возможности;
- Квалификацию и опыт персонала, вовлеченного в процесс управления рыночным риском.

7.6. Все это предполагает разработку 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.

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

- **Мероприятия по управлению рисками включают в себя:** доведение до органов управления Платежной организации соответствующей информации о рисках; определение показателей и порядка обеспечения бесперебойности функционирования Платежной организации; определение методик анализа рисков; определение порядка обмена информацией, необходимой для управления рисками; определения порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев; определение порядка изменения операционных и технологических средств и процедур; определение порядка обеспечения защиты информации в Платежной организации.
- **Способы управления рисками** в Платежной организации определяются такими способами как управление очередностью исполнения распоряжений должностными лицами; осуществление расчета, в пределах, предоставленных агентами Платежной организации денежных средств; осуществление расчетов в Платежной организации до конца рабочего дня; обеспечение возможности предоставления лимита; другими способами управления рисками.

8. Порядок урегулирования спорных ситуаций и разрешения споров с Клиентами

8.1. При наличии императивных норм законодательства, действующего на территории Республики Казахстан, исключающих применение договорных условий в отношениях, связанных с осуществлением деятельности Платежной организации, указанные императивные нормы имеют приоритет над условиями Правил.

8.2. Разногласия между Участниками платежа, связанные с осуществлением деятельности Платежной организации или расчетов между Участниками платежа, которые могут служить основанием для возникновения необходимости судебного рассмотрения споров между Участниками платежа и (или) перевода денег, рассматриваются Платежной организацией в претензионном порядке.

8.3. Претензия Участника платежа, изложенная в письменной форме на официальном бланке за подписью его уполномоченного должностного лица, направляется другой стороне заказной почтой или иным способом, подтверждающим вручение претензии адресату. Претензия должна быть заявлена в течение 10 (десяти) рабочих дней после возникновения основания для претензии, и содержать указание на обстоятельства, служащие основанием для ее предъявления, а также на дату возникновения указанных обстоятельств. Претензии, поступившие по истечению указанного срока, не рассматриваются.

8.4. Рассмотрение претензий включает в себя изучение обстоятельств, позволяющих установить исполнение (неисполнение) Участниками платежа своих функций и обязательств, вытекающих из настоящих Правил и договоров, заключенных с ними. Платежная организация вправе запрашивать у Участников платежа любую информацию, необходимую для выяснения указанных обстоятельств.

8.5. Решение по претензии должно быть принято в течение 15 (пятнадцати) календарных дней после получения претензии и направлено Участнику платежа в письменной форме.

8.6. При невозможности урегулирования разногласий в претензионном порядке споры разрешаются судом по месту нахождения Платежной организации в соответствии с законодательством Республики Казахстан.

9. Порядок соблюдения мер Информационной безопасности

9.1. AIRBA PAY обеспечивает создание и функционирование системы управления Информационной безопасностью, являющейся частью общей системы управления Платежной организации, предназначенной для управления процессом Обеспечения информационной безопасности.

9.2. Система управления Информационной безопасностью обеспечивает защиту Информационных активов Платежной организации, допускающую минимальный уровень потенциального ущерба для бизнес-процессов Платежной организации.

9.3. AIRBA PAY обеспечивает надлежащий уровень системы управления Информационной безопасностью, ее развитие и улучшение.

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

- раскрыта по требованию или с разрешения Участника платежа, являющегося владельцем данной информации;
- подлежит предоставлению третьим лицам в объеме, необходимом для исполнения обязательств, предусмотренных настоящими Правилами;
- требует раскрытия по основаниям, предусмотренным законодательством Республики Казахстан.

9.5. Не является нарушением конфиденциальности и безопасности Участников платежа предоставление конфиденциальной информации третьей стороне в целях исполнения Правил и иных соглашений Участников платежа; предоставление конфиденциальной информации по законному требованию правоохранительных и иных уполномоченных государственных органов, а также в других предусмотренных действующим законодательством Республики Казахстан случаях.

9.6. Оператор платежных систем обеспечивает бесперебойное функционирование системы AIRBA PAY в режиме 24/7/365 (24 (двадцать четыре) часа в день, 7 (семь) дней в неделю, 365 (триста шестьдесят пять) дней в году), за исключением времени проведения профилактических работ.

9.7. AIRBA PAY обеспечивает защиту информации о средствах и методах обеспечения Информационной безопасности, персональных данных и об иной информации, подлежащей обязательной защите в соответствии с законодательством Республики Казахстан, которая может стать ему известной в ходе осуществления деятельности Платежной организации.

9.8. AIRBA PAY в целях обеспечения конфиденциальности, целостности и доступности информации Платежной организации осуществляет следующие функции:

- 1) организует систему управления Информационной безопасностью, осуществляет координацию и контроль деятельности по Обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию Инцидентов информационной безопасности;
- 2) обеспечивает методологическую поддержку процесса Обеспечения информационной безопасности;
- 3) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля Информационной безопасности в рамках своих полномочий;
- 4) осуществляет сбор, консолидацию, хранение и обработку информации об Инцидентах информационной безопасности;
- 5) осуществляет анализ Информации об инцидентах информационной безопасности;
- 6) обеспечивает внедрение, надлежащее функционирование программно-технических средств, автоматизирующих процесс Обеспечения информационной безопасности, а также предоставление доступа к ним;

- 7) определяет ограничения по использованию привилегированных учетных записей;
- 8) организует и проводит мероприятия по обеспечению осведомленности работников Платежной организации в вопросах Информационной безопасности;
- 9) осуществляет мониторинг состояния системы управления Информационной безопасностью Платежной организации;
- 10) периодически (но не реже 1 (одного) раза в год) осуществляет информирование исполнительного органа Платежной организации о состоянии системы управления Информационной безопасностью Платежной организации;
- 11) поддерживает в актуальном состоянии схемы периметра защиты информационно-коммуникационной инфраструктуры и перечень администраторов средств обеспечения его безопасности;
- 12) устанавливает на периметре защиты информационно-коммуникационной инфраструктуры межсетевые экраны;
- 13) обеспечивает безопасность доступа пользователей к ресурсам сети Интернет из периметра защиты информационно-коммуникационной инфраструктуры.

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

9.10. 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. Участники платежа обязуются принимать все необходимые меры по сохранению конфиденциальности, предотвращению несанкционированного использования и защите идентификационных данных от несанкционированного доступа со стороны третьих лиц.

9.11. Платежная организация управляет рисками Информационной безопасности с указанием критериев приемлемого уровня по отношению к Информационным активам. При реализации рисков Информационной безопасности разрабатывается план мероприятий, направленный на минимизацию возникновения подобных рисков.

9.12. Информация об Инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по Обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению.

9.13. Срок хранения информации об Инцидентах информационной безопасности в Платежной организации составляет 5 (пять) лет.

9.14. Платежной организацией определяется порядок принятия неотложных мер к устранению Инцидента информационной безопасности, его причин и последствий.

9.15. В частности, в Платежной организации ведется журнал учета Инцидентов информационной безопасности с отражением всей информации об Инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.

9.16. Платежная организация предоставляет в Национальный Банк Республики Казахстан информацию о следующих выявленных Инцидентах информационной безопасности:

- 1) эксплуатация уязвимостей в прикладном и системном программном обеспечении;
- 2) несанкционированный доступ в информационную систему;
- 3) атака «отказ в обслуживании» на информационную систему или сеть передачи данных;
- 4) заражение сервера вредоносной программой или кодом;

5) совершение несанкционированного перевода денежных средств вследствие нарушения контролей Информационной безопасности;

6) Инцидентах информационной безопасности, несущих угрозу стабильности деятельности Платежной организации.

Информация об Инцидентах информационной безопасности, указанных в настоящем пункте, предоставляется Платежной организацией в возможно короткий срок, но не позднее 48 (сорока восьми) часов с момента выявления, в виде карты инцидента информационной безопасности по форме, составленной в соответствии с Постановлением Правления Национального Банка Республики Казахстан от «31» августа 2016 года № 215 «Об утверждении Правил организации деятельности платежных организаций».

Информация по обработанным Инцидентам информационной безопасности представляется в электронном формате с использованием платформы Национального Банка Республики Казахстан для обмена событиями и инцидентами информационной безопасности. На каждый Инцидент информационной безопасности заполняется отдельная карта инцидента информационной безопасности.

10. Описание программно-технических средств и оборудования, необходимого для оказания платежных услуг

10.1. Программное обеспечение Платежной организации обеспечивает:

1) надежное хранение информации, защиту от несанкционированного доступа, целостность баз данных и полную сохранность информации в электронных архивах и базах данных при полном или частичном отключении электропитания в любое время на любом участке оборудования;

2) многоуровневый доступ к входным данным, функциям, операциям, отчетам, реализованным в программном обеспечении, предусматривающим как минимум, два уровня доступа: администратор и пользователь;

3) контроль полноты вводимых данных полей обязательных к заполнению, необходимых для проведения и регистрации операций (при выполнении функций или операций без полного заполнения всех полей программа обеспечивает выдачу соответствующего уведомления);

4) поиск информации по критериям и параметрам, определенным для данной информационной системы, с сохранением запроса, а также сортировку информации по любым параметрам (определенным для данной информационной системы) и возможность просмотра информации за предыдущие даты, если такая информация подлежит хранению в информационной системе;

5) обработку информации и ее хранение по дате и времени;

6) автоматизированное формирование форм отчетов, представляемых Платежной организацией в Национальный Банк Республики Казахстан, а также отчетов о проведенных операциях;

7) ведение и автоматизированное формирование журналов системы внутреннего учета. Программное обеспечение формирует журнал полностью, а также частично (на указанный диапазон дат, определенную дату);

8) возможность резервирования и восстановления данных, хранящихся в учетных системах;

9) возможность вывода выходных документов на экран, принтер или в файл;

10) возможность обмена электронными документами;

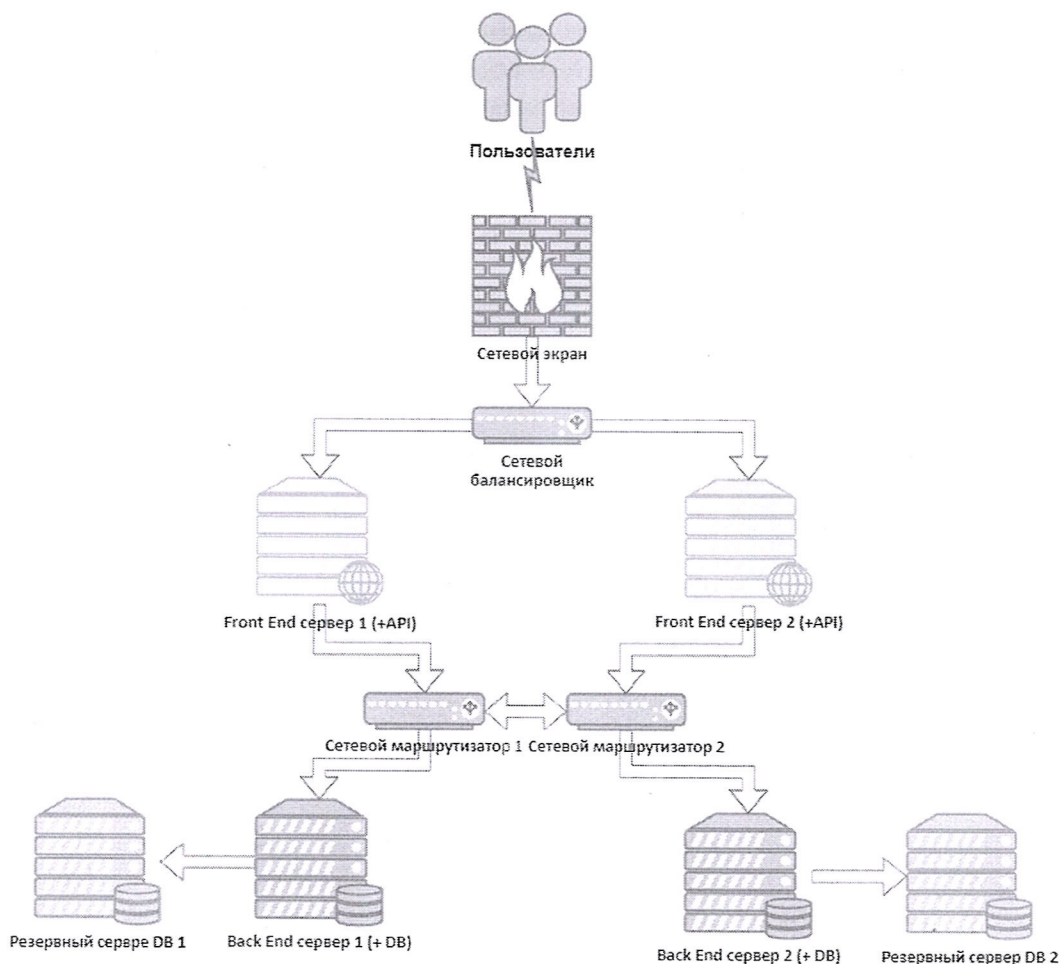
11) регистрацию и идентификацию происходящих в информационной системе событий с сохранением следующих атрибутов: дата и время начала события, наименование события, пользователь, производивший действие, идентификатор записи, дата и время окончания события,

результат выполнения события;

12) изменение паролей предустановленных учетных записей средств обеспечения безопасности периметра защиты информационно-коммуникационной инфраструктуры.

10.2. Техническая архитектура Платежной организации состоит из следующих компонентов:

Сервис разработан на микро-сервисной серверной технологии в основе языка программирования Go Lang, управляемого через Docker контейнеры с оркестрацией в Kubernetes. В качестве системы хранения данных используется MongoDB. Серверная структура AIRBA PAY состоит из сетевого балансировщика, двух идентичных серверов для обработки транзакций, сервера баз данных и резервных двух серверов баз данных, который также обеспечивает создание и хранение бекапов базы данных. Все серверы работают под управлением Ubuntu.



10.3. Отказоустойчивость:

Отказоустойчивость сервиса обеспечивается за счет распределения нагрузки между двумя серверами приложений. Эту функцию выполняет программное обеспечение Nginx для балансировки трафика пользователя «сетевой балансировщик», далее данные обрабатываются на frontend-сервере, проксирующего запросы к серверам приложений через программное обеспечение NARoxy в режиме Sticky-session. В случае недоступности одного из серверов (падение канала связи, высокая текущая нагрузка, выход сервера из строя) все запросы автоматически и без задержек на переключение перенаправляются на второй сервер, оставшийся в онлайн-режиме. Таким образом достигается баланс производительности серверов в базовом режиме работы и обеспечение бесперебойной обработки транзакций в случае непредвиденных

обстоятельств, когда один из серверов по каким-либо причинам временно выходит из строя. Серверы баз данных работают в Docker контейнерах с оркестрацией в Kubernetes режиме трех нодовой структуры, и в случае отказа работы основного сервера ноды обработки транзакций автоматически распределяются и исполняются на остальных нодах, при этом автоматически сервис понимает третий вышедший из строя согласно правилам оркестрации в Kubernetes.

10.4. Резервное копирование:

Резервное копирование сервера баз данных осуществляется встроенными средствами виртуальных машин с сохранением бекапов на резервном сервере баз данных в течение одного месяца. Схема копирования такова: каждый час + финальное в 1 час:00 минут с удалением ежечасных копий. Бекапы старше одного месяца удаляются в целях недопущения переполнения хранилища данных. Актуальность и сохранение кодовой базы системы обработки транзакций обеспечивается структурой управления CI/CD на базе GitLab. Непосредственно репозитории кода хранятся на сервисе GitLab, деплоймент с которого, в случае отказа серверов, может быть произведен в кратчайшие сроки.

10.5. Безопасность доступа к серверной инфраструктуре:

Административный доступ к любому из серверов возможен только при наличии 2048-битного SSH2-RSA-ключа. Получить доступ к серверной инфраструктуре перебором паролей или любым другим несанкционированным способом невозможно. Доступ Клиента в Личный кабинет, как и доступ администратора AIRBA PAY в кабинет управления транзакциями, осуществляется только посредством двухфакторной авторизации, которая предоставляется сервисом SSO. Авторизация на этом участке при помощи других, менее защищенных методов невозможна.

10.6. Безопасность проведения транзакций:

Каждая транзакция в сервисе AIRBA PAY проходит через фильтр безопасных платежей. Данный фильтр является высокоэффективной мерой защиты безопасности транзакций и обеспечивает высокий уровень защиты от мошенничества. Основываясь на аналитических данных по транзакциям, а также на алгоритмах машинного обучения сервис принимает решение о том, является ли транзакция мошеннической или нет. Фильтр безопасных платежей не требует наличия включенного 3DSecure или другого метода защиты безопасности транзакций, что позволяет сервису AIRBA PAY значительно расширить пользовательскую базу Плательщиков за счет абонентов, не имеющих или не включающих 3DSecure.

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

11. Порядок внесения изменений в Правила

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

11.2. В случае несогласия Участника платежа/Клиента с изменениями и/или дополнениями в Правила или тарифами, Участник платежа/Клиент вправе отказаться от дальнейшего использования сервисов Платежной организации.

11.3. Последующее внесение изменений и/или дополнений в Правила осуществляется в порядке, установленном настоящим разделом Правил.

11.4. Дальнейшее пользование услугами Платежной организации после вступления в силу любых изменений и/или дополнений в Правила означает согласие Участников платежа с такими изменениями и/или дополнениями.