Утверждены
Решением единственного участника
ТОО «EXXUS»
(№ 0003 от 25 января 2024г.)

ПРАВИЛА ОСУЩЕСТВЛЕНИЯ ДЕЯТЕЛЬНОСТИ
ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ ТОО «EXXUS»

2024 год

Оглавление

Глава 1. Общие положения
Глава 2. Термины и определения
Глава 3. Описание платежных услуг, оказываемых платежной организацией
Глава 4. Порядок и сроки оказания платежных услуг клиентам платежной организации
Глава 5. Стоимость платежных услуг (тарифы), оказываемых платежной организацией.
Глава 6. Порядок взаимодействия с третьими лицами, обеспечивающими технологическое обеспечение платежных услуг, оказываемых платежной организацией
Глава 7. Сведения о системе управления рисками, используемой платежной организацией
Глава 8. Порядок урегулирования спорных ситуаций и разрешения споров с клиентами
Глава 9. Порядок соблюдения мер информационной безопасности
Глава 10. Описание программно-технических средств и оборудования, необходимого для оказания платежных услуг
Глава 11. Заключительные положения

ГЛАВА 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящие Правила осуществления деятельности платежной организации Товарищества с ограниченной ответственностью «EXXUS» (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 (далее – Правила 215), Постановлением Правления Национального Банка Республики Казахстан от 31 августа 2016 года № 205 «Об утверждении Правил выпуска платежных карточек, а также требований к деятельности по обслуживанию операций с их использованием на территории Республики Казахстан» (далее – Правила № 205), Уставом ТОО «EXXUS» и определяют порядок организации деятельности ТОО «EXXUS» в качестве платежной организации.

1.2. Товарищество с ограниченной ответственностью «EXXUS» (далее по тексту – Товарищество, Платежная организация и(или) как указано в тексте в соответствии с используемой терминологией) при наличии регистрационного номера учетной регистрации платежной организации, присвоенного Национальным Банком Республики Казахстан, оказывает следующие виды платежных услуг:

1) услуги по приему наличных денег для осуществления платежа без использования банковского счета отправителя денег;

2) услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, филиалу банка-нерезидента Республики Казахстан, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам.

ГЛАВА 2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящих Правилах используются понятия, предусмотренные законами Республики Казахстан «О платежах и платежных системах», от 31 августа 1995 года «О банках и банковской деятельности в Республике Казахстан», от 7 января 2003 года «Об электронном документе и электронной цифровой подписи», от 28 августа 2009 года «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», от 21 мая 2013 года «О персональных данных и их защите», Правилами №215, Правилами №205 , а также следующие понятия употребляются в значениях, указанных ниже в разрезе оказания платежных услуг:

2.1.1. В рамках оказания платежных услуг по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег

1. Агент (Платежный агент) – юридическое лицо или индивидуальный предприниматель, заключившие с банком или организацией, осуществляющей отдельные виды банковских операций, или платежной организацией агентский договор по оказанию платежных услуг.

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

3. **Получатель платежа или Поставщик услуг** – 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/Работы/Услуги, либо физическое лицо, принимающее деньги от Клиента, не связанные с предпринимательской деятельностью.

4. **Клиент** – физическое лицо, обладающее надлежащей дееспособностью в соответствии с законодательством Республики Казахстан для осуществления Платежа, совершившее конклюдентные действия, направленные на заключение Договора об оказании услуг, и обладающее Аутентификационными данными для доступа к Системе в целях управления своей Учетной записью, и последующего оказания Платежной организацией платежных услуг, предусмотренных Правилами.

5. **Система по учету платежей (далее – «Система»)** – совокупность программно-технических средств Платежной организации, обеспечивающих информационно-технологическое взаимодействие и регистрацию платежей.

6. **Субагент (Платежный субагент)** – юридическое лицо или индивидуальный предприниматель, заключившие с платежным агентом агентский договор по оказанию платежных услуг.

7. **Товар** – товары, работы, услуги, права на результаты интеллектуальной деятельности, реализуемые Получателями платежа конечным потребителям (Клиентам) для личного, семейного или домашнего использования.

8. **Пункт приема Платежей (ППП)** - территория, на которой Платежная организация, в том числе через своих Агентов и Субагентов, осуществляет прием платежей с использованием, касс, специализированных кассовых устройств,

терминалов самообслуживания (специализированных автоматов по приему платежей), а также область пространства сети Интернет, в которой Платежная организация, ее Агент/Субагент осуществляет прием платежей с использованием специализированного программного обеспечения.

2.1.2. В рамках оказания платежной услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, филиалу банка-нерезидента Республики Казахстан, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам:

1) **АПК** – специализированный аппаратно-программный комплекс Платежной организации, Банка.

2) **Банк** – банк второго уровня, с которым Платежная организация заключила договор в целях оказания услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам.

3) **Возвратный платеж** – требование банка эмитента в отношении транзакции, составленное в соответствии с Правилами Международных платежных систем (МПС), включая первое и все дальнейшие требования в отношении одной Транзакции.

4) **Данные транзакции** – информация о транзакции и платежной карточке, с помощью которых была проведена транзакция, а также информация о результатах идентификации держателя платежной карточки.

5) **Держатель платежной карточки (Покупатель)** – владелец платежной карточки, использующий ее для совершения платежной услуги.

6) **Итоговый реестр платежей** – отчет в электронном виде, формируемый Платежной организацией и содержащий перечень всех платежей с указанием сумм за каждый календарный день (или дни, в случае если Итоговый реестр формируется за несколько выходных/нерабочих праздничных дней). Формат Итогового реестра платежей определяется Платежной организацией самостоятельно.

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

8) **Мерчант** – предприятие торговли (услуг), которое принимает к оплате платежные карточки.

9) **Международные платежные системы (МПС)** – международные платежные системы: Visa International и MasterCard International и другие МПС.

10) **Мошенническая транзакция** – транзакция, проведенная с использованием поддельной, украденной или утерянной платежной карточки, умышленно искаженных данных платежной карточки, либо транзакция, проведенная другим незаконным способом.

11) **Обработка Операций (Процессинг)** – обработка в соответствии с Правилами МПС, Платежной организацией и Банком с применением АПК, информации об Операциях, которая включает в себя сбор, обработку и рассылку участникам расчетов (эквайер, мерчант, держатель платежной карточки) информации по совершенным Операциям.

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

13) **Операция оплаты** – оплата покупателем услуг Мерчанта в Интернет-магазине либо иных способов с использованием платежной карточки.

14) **Операция отмены оплаты** – инициированная одной из сторон отмена ранее произведенной Операции оплаты в связи с ошибкой или техническим сбоем при ее проведении.

15) **Операция возврата** – операция по возврату денег Покупателю по проведённой Покупателем Операции оплаты, в связи с его отказом от Услуги (возвратом товара) Мерчанта, инициированная Мерчантом. Операция возврата осуществляется исключительно с использованием платежной карточки, по которой Покупателем ранее была совершена Операция оплаты. Выдача наличных денег в случае возврата товара, ранее оплаченного с использованием платежной карточки, запрещается.

16) **Одностадийная авторизация** – Операция оплаты, при которой сумма платежа одномоментно списывается с платежной карточки Покупателя (клиента).

17) **Двустадийная авторизация** – Операция оплаты, при которой сумма платежа на первой стадии резервируется (холдируется) на счете, к которому выпущена платежная карточка Покупателя, а на второй стадии, после подтверждения Авторизации Мерчантом, списывается с платежной карточки Покупателя.

18) **Операция отмены возврата** – отмена ранее произведенной Операции возврата, инициированная Мерчантом.

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

20) **Транзакция** – операция с платежной карточкой, в результате которой производится оплата каких-либо товаров или услуг.

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

22) **Система** – совокупность программно-технических средств, документации и организационно-технических мероприятий, обеспечивающих информационно-технологическое взаимодействие, регистрацию и осуществление платежей и иных операций в соответствии с настоящими Правилами осуществления деятельности платежной организации ТОО «EXXUS».

ГЛАВА 3. ОПИСАНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

3.1. Услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег оказываются Платежной организацией на основании договоров, заключаемых Платежной организацией с Получателями платежа – поставщиками Товаров, условиями которых предусмотрена возможность привлечения к оказанию платежных услуг платежных агентов/субагентов на основании агентских/субагентских договоров по оказанию платежных услуг, заключаемых между Платежной организацией и платежным агентом, между платежными агентами и платежными субагентами (в случае привлечения платежного субагента). Договор размещается на сайте Платежной организации или в пунктах приема платежей. Услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег оказывается посредством внесения плательщиком наличных денег через терминалы, принадлежащие платежным агентам/субагентам. В приложениях №2 и №3 к Правилам, указаны характеристики и требования к электронным терминалам.

3.2. услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, филиалу банка-нерезидента Республики Казахстан, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам, оказываются Платежной организацией на основании отдельных договоров, заключенных с банком/ банками второго уровня и платежной организацией с третьими лицами и 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, с которым заключен соответствующий договор, а банк, в свою очередь, исполняет указание Клиента, переданное через Платежную организацию в электронной форме.

ГЛАВА 4.
ПОРЯДОК И СРОКИ ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ КЛИЕНТАМ ПЛАТЕЖНОЙ ОРГАНИЗАЦИИ

4.1. Порядок оказания услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег.

4.1.1. Прием наличных денег для осуществления платежа без открытия банковского счета отправителя денег в пользу поставщиков услуг происходит путем внесения физическим лицом денег через ППП самой Платежной организации и (или) платежного агента/субагента. По окончании платежа выдается документ, подтверждающий платеж, соответствующий требованиям законодательства Республики Казахстан.

Оказание платежными агентами/субагентами платежной услуги по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег, происходит в следующем порядке:

1) Платежный агент/субагент заключает с Платежной организацией (либо как с платежным агентом) договор об оказании платежных услуг.

2) Платежный агент/субагент проходит регистрацию в Системе по учету платежей, с присвоением ID, для чего:

– в согласованный сторонами договора срок агент/субагент осуществляет реализацию Интерфейса подключения (API) для Агента к Системе Платежной организации, либо по договоренности сторон Платежная организация осуществляет реализацию технического протокола;

– стороны проводят техническое тестирование систем;

– сторонами определяется техническая готовность систем к отправке агентом/субагентом информации о платежах Платежной организации.

3) Оказание платежной услуги обеспечивается по соглашению сторон заключенного договора предоставлением платежным агентом/субагентом гарантийного взноса (авансового платежа, предварительного возмещения) на планируемый объем платежей. Для этого Платежной организацией создается авторизационный доступ с отражением расчетного баланса в Системе платежного агента/субагента для учета сумм принятых платежей и комиссий. При совершении платежа клиентом через ППП платежного агента/субагента, сумма принятых платежей автоматически списывается с расчетного баланса агента в Системе Платежной организации.

4) Платежный агент/субагент обязуется обеспечивать на счете неснижаемый остаток денег, достаточный для исполнения обязательств перед Платежной организацией, если данное условие предусмотрено положениями договора.

5) При отсутствии в день приема платежей денег в остатке гарантийного взноса платежного агента/субагента, обязательство платежного агента/субагента является необеспеченным, и Платежная организация вправе приостановить исполнение договора либо предоставить платежному агенту/субагенту отсрочку в перечислении платежа (коммерческий кредит либо овердрафт) на основании отдельного соглашения, заключаемого Платежной организацией с платежным агентом/субагентом, или гарантийного письма.

6) Платежный агент/субагент обязан передавать Системе данные о каждом принятом платеже для внесения изменений в лицевой счет Плательщика поставщиком услуг. Сведения должны быть переданы непосредственно в период приема платежа на основании данных, указываемых клиентом, без ошибок и искажений.

7) Каждой операции по передаче данных о платеже присваивается уникальный номер в Системе Платежной организации. Сочетание аутентификационных данных платежного агента/субагента – логин, пароль и/или ID в Системе признаются сторонами в качестве однозначного и бесспорного подтверждения совершенного платежа.

8) После приема платежа платежный агент/субагент обязан выдать клиенту квитанцию, или электронное подтверждение использования ППП платежного агента/субагента для передачи данных о платеже, содержащую информацию, установленную Законом о платежах и платежных системах, Правилами № 215.

9) Также сторонами в договоре может быть предусмотрено оказание платежных услуг без предварительного возмещения, в порядке последующего перечисления/перевода сумм принятых платежей на периодической основе.

10) Платежный агент обеспечивает передачу информации о каждом принятом платеже Платежной организации в режиме реального времени в соответствии с протоколом технического взаимодействия сторон, при этом по мере передачи Платежной организации информации о принятых платежах, сумма таких распоряжений автоматически уменьшает сумму остатка гарантийного взноса, которое засчитывается в счет исполнения обязательств агента по перечислению Платежной организации суммы принятых платежей.

11) При приеме платежей платежным агентом/субагентом может взиматься комиссия с платежа, плательщика. Размер комиссии устанавливается Платежной организацией и в пределах допустимых комиссий, согласованных соответствующим договором, между Платежной организацией и поставщиком услуг.

12) Платежная организация с контрагентами (агентами и поставщиками услуг) проводит сверку данных с использованием Личного кабинета контрагента, предоставляемого Платежной организацией, после установления деловых отношений.

13) на ежедневной основе осуществляет мониторинг Реестра Платежей, отражаемого в Личном кабинете Агента, проводит сверку Реестра Платежей с данными своей системы. В случае наличия расхождений, но не позднее 1 (одного) рабочего дня с даты обнаружения, уведомляет Платежную организацию путем направления уведомления по электронной почте либо в письменной форме. По получению уведомления от Агента, Стороны согласовывают информацию, и принимают решение, обязательное для обоих Сторон, о порядке учета оспариваемых транзакций при проведении сверки.

Порядок взаимодействия Платежной организации с Поставщиками услуг

1) Платежная организация заключает с Поставщиком услуг договор поручения об оказании платежных услуг, который должен содержать следующую информацию:

- порядок зачисления денег с банковского счета платежной организации на банковский счет поставщика услуги;
- права и обязанности сторон;
- порядок вознаграждения Платежной организации за оказание платежной услуги;
- условия привлечения Платежной организации к оказанию платежной услуги, а также привлечение Платежной организацией Агентов/Субагентов.

2) Оказание платежной услуги обеспечивается по соглашению сторон заключенного договора предоставлением Платежной организации авансового платежа на планируемый объем платежей. Для этого Платежной организации создается авторизационный доступ с отражением расчетного баланса в Системе Платежной организации для учета сумм принятых платежей и комиссий. При совершении платежа клиентом через ППП Платежной организации и (или) платежного агента/субагента, сумма принятых платежей автоматически списывается с расчетного баланса Платежной организации.

3) Платежная организация обязуется обеспечивать на счете неснижаемый остаток денег, достаточный для исполнения обязательств перед Поставщиком услуг.

4) При отсутствии в день приема платежей денег в остатке авансового платежа платежной организации, обязательство платежной организации является необеспеченным, и Поставщик услуг вправе приостановить исполнение договора либо предоставить Платежной организации отсрочку в перечислении платежа (коммерческий кредит либо овердрафт) на основании отдельного соглашения, заключаемого Платежной организацией с Поставщиком услуг, или гарантийного письма.

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

6) Каждой операции по передаче данных о платеже присваивается уникальный номер (референс) в Системе Платежной организации.

7) Также сторонами в договоре может быть предусмотрено оказание платежных услуг без предварительного возмещения, в порядке перечисления/перевода сумм принятых платежей на периодической основе.

8) Платежная организация обеспечивает передачу информации о каждом принятом платеже Поставщику услуг в режиме реального времени в соответствии с протоколом технического взаимодействия сторон, при этом по мере передачи Поставщику услуг информации о принятых платежей, сумма таких распоряжений автоматически уменьшает сумму остатка авансового платежа, которое засчитывается в счет исполнения обязательств Платежной организации по перечислению Поставщику услуг суммы принятых платежей.

9) При приеме платежей Платежной организацией взимается комиссия с платежа. Размер комиссии устанавливается поставщиками услуг.

10) Платежная организация с контрагентами (агентами и поставщиками услуг) проводит ежедневную сверку.

11) На ежемесячной основе производится сверка взаиморасчетов, на основании которой Платежная организация предоставляет подписанный со своей стороны отчет Платежной организации о принятых платежах или акт сверки и(или) акт выполненных работ и(или) счет-фактуру на сумму вознаграждения, на основании которого происходит сверка взаиморасчетов (в случае, если сторонами договора достигнута договоренность по предоставлению указанных документов).

Сроки оказания платежных услуг – от 10 минут, но не более 24 часов с момента внесения платежа.

4.2. Порядок оказания услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, филиалу банка-нерезидента Республики Казахстан, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам (далее - Услуги).

4.2.1. **Порядок подключения Мерчанта к Системе:**

Для подключения к Системе, Мерчанту необходимо направить заявление в адрес Платежной организации либо на Сайте подать заявку на подключение с содержанием адреса веб-сайта Мерчанта, номера телефона и электронного адреса контактного лица Мерчанта. После проведения проверки пакета документов, представленных Мерчантом и подписания договора, в Системе создается личный кабинет Мерчанта (ЛК).

Требования к сайту Мерчанта:

- URL-адрес и все внутренние ссылки сайта Мерчанта должны быть рабочими и адекватно обрабатываемыми;
- сайт Мерчанта не должен предоставлять услуги «развлечений для взрослых» («Adult Entertainment»);
- на электронной витрине сайта Мерчанта не должно быть ссылок или баннеров подозрительных сайтов (например, сайтов для взрослых и т.п.), а также ссылок баннерных сетей, в которых могут всплыть баннеры подозрительного содержания.
- сайт не должен располагаться на бесплатных серверах, предоставляющих услуги хостинга.

- наличие на сайте актуальной справочной информации о Мерчанте. Обязательным условием является наличие наименования страны, адреса места нахождения, адреса для корреспонденции (адрес не может быть до востребования), а также контактных телефонов, по которым клиент может связаться со службой поддержки сайта.

- перечень продаваемых товаров (работ, услуг), перечисленных в анкете Мерчанта, должен соответствовать перечню товаров (работ, услуг), предлагаемых на сайте.

- полнота описания потребительских характеристик продаваемых товаров (работ, услуг). (Проверяется для того, чтобы недостаток описания товара, работы, услуги не мог стать причиной для возврата платежа). В том числе, в обязательном порядке на сайте должны быть указаны цены на товары, работы, услуги.

- реквизиты платежной карточки не должны приниматься на сайте. Для оплаты с использованием платежной карточки клиент должен обязательно переадресовываться на Систему Платежной организации.

- 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 платежных карточек, и переадресация клиента на Сайт Системы.

- 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.

- наличие на сайте описания процедур возврата денег, предоставления взаимозаменяемых товаров, обмена товаров и т.п. при отказе от товара (работы, услуги). В случае если такие процедуры Мерчантом не предусмотрены, то он обязан информировать об этом на своем сайте.

- Мерчант обязан предусмотреть осуществление контроля получения заказов клиентами.

- Мерчант обязан предусмотреть методы ограничения и контроля рисков мошеннических операций.

- все страницы, которые связаны с работой сайта, должны находиться под единым доменным именем.

- наличие предупреждения о том, что посещение сайта, приобретение и доставка клиента конкретного товара (работы, услуги) могут быть незаконными на территории страны, где находится клиент.

- наличие предупреждения о том, что клиент несет ответственность за невыполнение законов своей страны при посещении данного сайта и попытке приобрести товары (работы, услуги), если таковые запрещены законодательством на территории страны, где он находится.

Мерчант представляет следующий пакет документов, подписанные уполномоченным лицом Мерчанта и заверенные печатью (при наличии), при необходимости Платежная организация оставляет за собой право запросить дополнительные документы:

Для юридических лиц

- для юридических лиц-резидентов и нерезидентов Республики Казахстан и их обособленных подразделений (филиалов и представительств):

- документ, выданный уполномоченным органом, подтверждающим факт прохождения государственной регистрации (перерегистрации) юридического лица;

- документы, удостоверяющие личность либо подтверждающие факт прохождения государственной регистрации (перерегистрации) учредителей (участников) юридического лица (за исключением документов учредителей (участников) акционерных обществ, а также хозяйственных товариществ, ведение реестра участников которых осуществляется единым регистратором), а также документы, удостоверяющие личность бенефициарных собственников юридического лица (за исключением случаев, когда бенефициарный собственник является учредителем (участником) юридического лица и выявлен на основании выписки из реестра акционеров (участников);

- документы, подтверждающие полномочия должностного(-ых) лица (лиц) лиц, на совершение действий от имени клиента без доверенности, в том числе на подписание документов юридического лица на совершение операций с деньгами и (или) иным имуществом;

Для индивидуальных предпринимателей

- для физических лиц - резидентов Республики Казахстан, осуществляющих индивидуальную предпринимательскую деятельность:

- документ, удостоверяющий личность;

- документ, выданный уполномоченным органом, подтверждающий факт прохождения государственной регистрации;

- нотариально заверенная доверенность на право подписи Договора уполномоченным лицом в случае, если Договор не подписывается индивидуальным предпринимателем.

Оказание платежной услуги обеспечивается по соглашению сторон на основании заключенного договора между Платежной организации и Мерчантом, который содержит следующие существенные условия:

- ✓ виды и общая характеристика оказываемых платежных услуг;
- ✓ порядок и максимальный срок оказания платежной услуги;

- ✓ размеры взимаемых сборов и комиссий или указание интернет-ресурса, содержащего данную информацию, и порядок их взимания;
- ✓ порядок предоставления информации о платежной услуге, в том числе направления Итогового реестра платежей;
- ✓ порядок защитных действий от несанкционированных платежей;
- ✓ порядок определения обменного курса, применяемого при оказании платежной услуги в иностранной валюте;
- ✓ условия, при которых поставщик платежных услуг оставляет за собой право на отказ в оказании платежной услуги;
- ✓ порядок регулирования вопросов по несанкционированным платежным услугам;
- ✓ право клиента на расторжение договора;
- ✓ порядок предъявления претензий и разрешения спорных ситуаций;
- ✓ порядок и размеры выплат по возмещению ущерба за необоснованный отказ от исполнения либо ненадлежащее исполнение указания.

После подписания договора происходит техническая интеграция Мерчантов с АПК Платежной организации.

Платежной организацией оказываются Услуги способом приема платежей от Клиентов по платежным карточкам Visa, MasterCard и других МПС.

Порядок приема платежей Клиентов по платежным карточкам Visa, MasterCard и других МПС:

1) Клиент Мерчанта со страницы его сайта переходит на страницу оплаты в Системе.

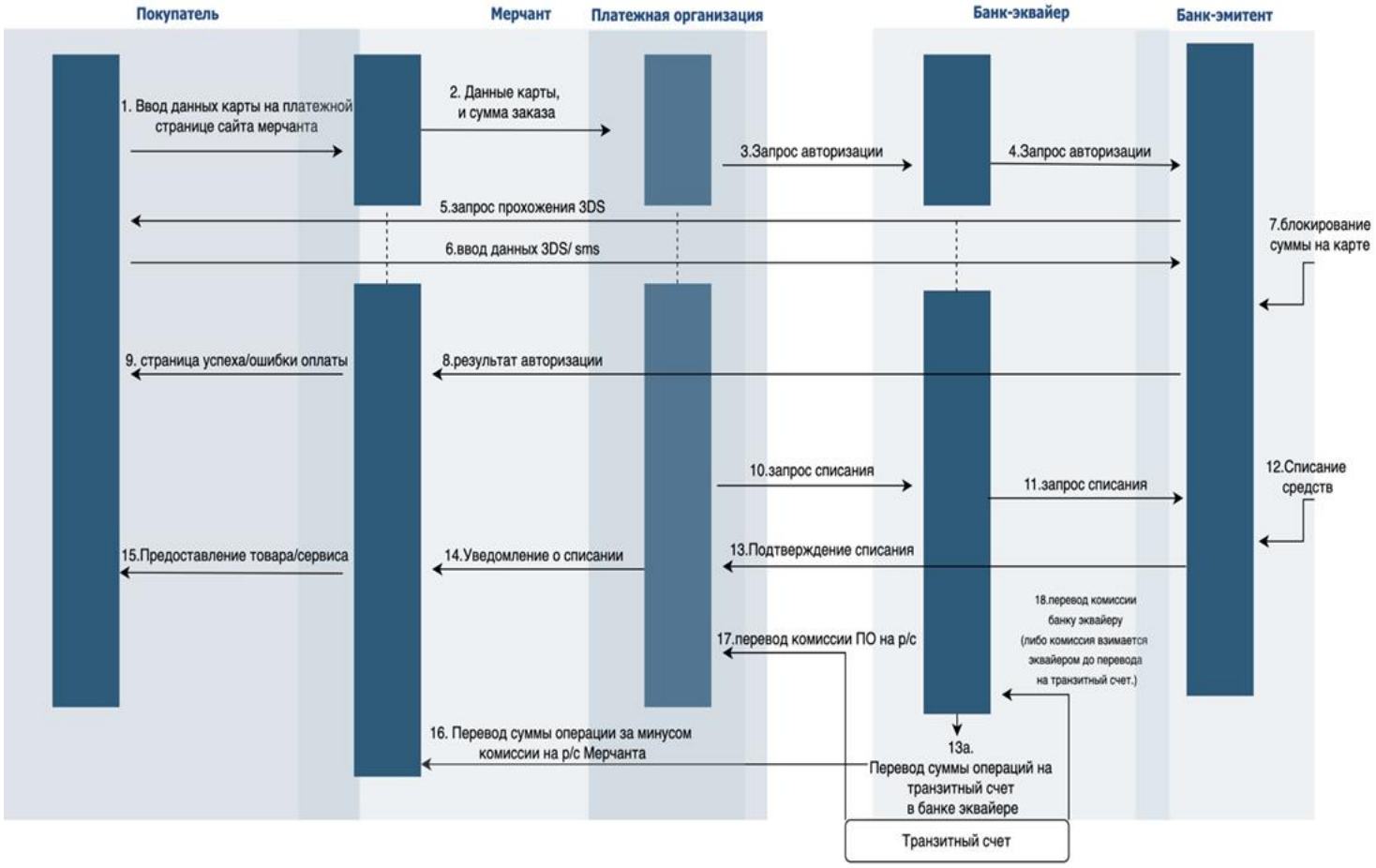
2) Клиент Мерчанта вводит реквизиты платежной карточки (тип платежной карточки, имя держателя платежной карточки, номер, срок действия, CVV).

Оказание Услуги по типу авторизации (при выборе Мерчантом):

- **одностадийная**, Платежная организация передает Банку информацию о списании заявленной суммы с платежной карточки плательщика, после чего Банк – эквайер передает информацию Банку – эмитенту, Банк - эмитент списывает сумму с платежной карточки клиента, далее Банк – эквайер зачисляет сумму на расчетный счет Мерчанта.

- **двустадийная**, Платежная организация передает Банку информацию о блокировке указанной суммы и Банк/Банк – эквайер блокирует сумму на платежной карточке клиента Мерчанта. Далее, если Мерчант подтверждает операцию, в этом случае Платежная организация передает Банку информацию о списании указанной суммы с платежной карточки клиента Мерчанта и Банк/Банк эквайер передает информацию Банку – эмитенту, Банк - эмитент списывает сумму с платежной карточки клиента Мерчанта. Платежная организация получает от Банка подтверждение исполнения Операции, и выдает Клиенту электронный чек, подтверждающий совершение Клиентом операции. При не подтверждении Мерчантом операции. Платежная организация не передает информацию о списании суммы Банку и Банк- эмитент не списывает сумму с платежной карточки клиента Мерчанта**.**

Схема информационных и денежных потоков при оказании Услуги



Детализированное описание передвижения денег с Мерчантом:

инициирование платежа: Держатель платежной карточки в целях оплаты за Товары/Услуги на сайте Мерчанта выбирает сервис-платежное решение, представленное ТОО «EXXUS» «оплатить платежной карточкой»;

переход с сайта Мерчанта на платежную страницу: после выбора производится переключение на платежную страницу АПК «EXXUS»;

заполнение реквизитов: на платежной странице Держатель платежной карточки осуществляет заполнение реквизитов платежной карточки для осуществления платежа. АПК осуществляет обработку информации с дальнейшей ее передачей в сторону Банка для проведения платежа. В случае необходимости ввода 3D SecureCode/SMS Code клиент перенаправляется на страницу Банка-эмитента Платежной карточки для ввода 3D SecureCode/SMS Code. В случае отсутствия у Банка-эмитента требования по вводу 3D SecureCode/SMS Code Банк осуществляет обработку транзакции;

Введение 3D SecureCode/SMS Code: по результатам успешного ввода клиентом 3D SecureCode/SMS Code либо в случае отсутствия у Банка-эмитента требований по 3D SecureCode/SMS Code Банк осуществляет обработку транзакции;

По итогам операционного дня Платежная организация направляет реестр платежей Банку для завершения расчетов с Мерчантами (перевод денег на банковский счет Мерчанта Банком-эквайером) и распределения комиссии между Банком и Платежной организацией. По операциям, проведенным в течение предыдущего операционного дня, Платежная организация направляет отчетный реестр Мерчанту по платежам, проведенным в его пользу.

В случае возврата товара/отказа Покупателем от Услуги, либо необходимости проведения отмены ранее осуществленной Операции оплаты, Мерчант инициирует проведение Операции возврата в ЛК либо действует согласно положениям заключенного с Платежной организацией договора (в случае если договором определен иной порядок действий).

Платежная организация обеспечивает хранение информации в электронном виде по всем совершенным операциям в течение 5-ти лет от даты прекращения деловых отношений с Мерчантом.

Платежная организация на периодической основе - один раз в сутки, и в соответствии с Правилами МПС осуществляет Обработку Операций, совершенных с момента предыдущего цикла Обработки Операций.

Обмен информацией осуществляется Платежной организацией с Банком, Мерчантом в соответствии с положениями соответствующих договоров. По результатам обработки Операций за Операционный день Платежная организация направляет отчет.

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

4.2.3. **Подтверждение оказания платежных услуг Клиенту:**

В качестве подтверждения оказания платежной услуги Клиенту, Платежная организация посредством Системы формирует и направляет Клиенту квитанцию, в электронном виде, на электронный адрес Клиента или путем SMS сообщения на номер телефона Клиента. Квитанция в обязательном порядке должна содержать информацию, установленную Законом о платежах и Правилами № 215. Допускается проставление Платежной организацией в документе, подтверждающем факт оказания платежной услуги, дополнительных реквизитов по оказанной платежной услуге.

ГЛАВА 5.

СТОИМОСТЬ ПЛАТЕЖНЫХ УСЛУГ (ТАРИФЫ), ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

Виды, размер, порядок взимания комиссий определяется сторонами Договора при оказании Платежной организацией услуг в соответствии с требованиями Закона о платежах, исходя из действующих рыночных тарифов на услуги подобного вида, с учетом сумм комиссий, подлежащих в последующем перечислению третьим лицам (агентам, субагентам, поставщикам услуг, лицам, обеспечивающим информационно-технологическое взаимодействие с Платежной организацией при оказании последними услуг).

По согласованию с агентом Платежная организация в договорах вправе включить положение о взимании комиссии системы, которая взимается с каждого платежа платежной организацией за прием денег в пользу поставщиков услуг и за обеспечение информационно-технологического взаимодействия в системе платежной организации, указываемая в процентном соотношении или в фиксированной денежной сумме в Приложениях к договорам.

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

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

Платежная организация при оказании платежных услуг, в том числе через платежных агентов, субагентов обеспечивает ознакомление плательщиком, Клиентом с размером взимаемой комиссии до осуществления платежа в денежном выражении.

Услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, филиалу банка-нерезидента Республики Казахстан, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам оплачиваются Мерчантом согласно положениям соответствующего договора. Также положениями договора может быть предусмотрена комиссия, подлежащая взиманию.

Стоимость услуг по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег указана в Приложении № 1 к настоящим Правилам.

Стоимость услуги по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, филиалу банка-нерезидента Республики Казахстан, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам определяется в зависимости от тарифов банка-эсквайра и составляет до 5% с каждой транзакции.

ГЛАВА 6.

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ТРЕТЬИМИ ЛИЦАМИ, ОБЕСПЕЧИВАЮЩИМИ ТЕХНОЛОГИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПЛАТЕЖНЫХ УСЛУГ, ОКАЗЫВАЕМЫХ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

6.1. Третьи лица – физические лица, индивидуальные предприниматели и юридические лица, Банк с которыми Платежная организация взаимодействует в рамках, заключенных между Платежной организацией и последними Договоров.

6.2. **Порядок взаимодействия при работе с поставщиками услуг.**

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

Ответственным сотрудником 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 определяется предполагаемая платежная нагрузка на Клиентов.

3) После проведения вышеуказанных действий и принятия положительного решения по согласованию со структурными подразделениями Платежной организации 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 пр.

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.

6.3. Заключение договора с Поставщиком услуг.

1) После осуществления действий, определенных подпунктом 3) п.6.2 настоящих Правил между Платежной организацией и Поставщиком услуг заключается Договор.

2) Платежной организацией заключается агентский договор с Поставщиком услуг об оказании платежных услуг (договор поручения) с обязательным наделением правом Платежной организации о принятия платежа в пользу Поставщика услуг, с использованием шаблонов Платежной организации, принимаемых в качестве образца, текст и содержание которого подлежит согласованию с контрагентом.

3) По согласованию сторон может быть использована форма договора, используемого при осуществлении текущей деятельности контрагентом.

4) Принимая во внимание, если стороны договора являются резидентами различных государств, стороны проводят согласование положений договора, с учетом требований законодательств обеих сторон.

5) Платежная организация осуществляет регистрацию Поставщика услуг в Системе, с присвоением ID.

6) Оказание платежной услуги обеспечивается предоставлением Платежной организацией гарантийного взноса (авансового платежа) на планируемый объем принятия платежей. При совершении платежа плательщиком через терминал (устройство) платежного агента/субагента Платежной организации, сумма принятых платежей списывается с расчетного счета (баланса) в системе Поставщика услуг.

7) Положениями договора по требованию Поставщика услуг может быть предусмотрена обязанность Платежной организации обеспечивать на указанном счете в системе Поставщика неснижаемый остаток денег, достаточный для исполнения обязательств перед Поставщиком услуг.

8) При отсутствии в день приема платежей денег в остатке гарантийного взноса Платежной организации, обязательство Платежной организации является необеспеченным, и Поставщик услуг вправе приостановить исполнение договора либо предоставить Платежной организации отсрочку в перечислении платежа (коммерческий кредит, либо овердрафт) на основании отдельного соглашения, заключаемого платежной организацией с поставщиком услуг или гарантийного письма.

9) 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.

10) Каждая операция по передаче данных о платеже сопровождается подписанием платежным агентом/субагентом электронного документа, форма которого согласована с соответствующим поставщиком услуг. Сочетание аутентификационных данных – логин, пароль и/или номер терминала в Системе - определены как аналог собственноручной подписи (далее АСП) Платежной организации и признаются сторонами в качестве однозначного и бесспорного подтверждения совершенного платежа.

11) Также по инициативе Поставщика услуг стороны договора могут утвердить иной порядок расчетов – перечисление платежной организацией сумм платежей плательщиков по факту с определенной периодичностью (постоплата).

12) При приеме платежей Платежной организацией, Агентом и Субагентом взимается комиссия с платежа, размер и порядок взимания которой, устанавливается исходя из действующих тарифов и условий, заключенных между Платежной организацией и поставщиками услуг Договоров.

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

ГЛАВА 7. СВЕДЕНИЯ О СИСТЕМЕ УПРАВЛЕНИЯ РИСКАМИ, ИСПОЛЬЗУЕМОЙ ПЛАТЕЖНОЙ ОРГАНИЗАЦИЕЙ

7.1. Система управления рисками представляет собой систему организации, политик, процедур и методов, принятых Платежной организацией с целью своевременного выявления, измерения, контроля и мониторинга рисков, для обеспечения её финансовой устойчивости и стабильного функционирования.

7.2. В целях организации деятельности по управлению рисками Платежная организация разрабатывает и утверждает внутренние документы в области управления рисками. Внутренние документы могут детализировать принципы управления рисками, а также содержать дополнительные мероприятия и способы управления рисками.

7.3. 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 лицо, в соответствии с Приказом работодателя или должностной инструкцией), 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.

7.4. Платежная организация проводит мероприятия для предотвращения возможных потерь и убытков в результате возникновения рисков, связанных и не связанных с осуществлением текущей (операционной) деятельности, требующих установления контроля (операционный, правовой, репутационный, риски в сфере ПОД/ФТ).

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

7.6. 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.

7.7. 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.

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

7.9. 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.

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

7.11. 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.

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

Мероприятия по управлению рисками:

1) определение организационной структуры управления, 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 руководящего состава Платежной организации соответствующей информации о рисках;
4) определение порядка обмена информацией, необходимой для управления рисками;
5) определение порядка взаимодействия в спорных, нестандартных и чрезвычайных ситуациях, включая случаи системных сбоев; определение порядка изменения операционных и технологических средств и процедур;
6) определение порядка оценки качества функционирования операционных и технологических средств, информационных систем;
7) определение порядка обеспечения защиты информации в Платежной организации.

7.13. Способы управления рисками в Платежной организации определяются с учетом особенностей деятельности Платежной организации, модели управления рисками.

7.14. Способы управления рисками:

1) установление обеспечительного взноса, суммы предварительного возмещения агентов и субагентов Платежной организации в рамках оказываемых платежных услуг;

2) автоматизированное управление очередностью исполнения распоряжений/указаний клиентов;

3) осуществление расчета до конца рабочего дня или в соответствии с установленным в Системе порядком;

4) осуществление расчета в пределах, предоставленных агентами Платежной организации денег;

5) обеспечение возможности установления лимита;

6) другие способы управления рисками по усмотрению Платежной организации.

7.15. Товарищество разрабатывает Программу управления рисками в соответствии с требованиями действующего законодательства Республики Казахстан содержащейся в Правилах внутреннего контроля в целях противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма, в соответствии с которой на ежегодной основе осуществляет оценку степени подверженности услуг (продуктов) ТОО «EXXUS» рискам отмывания доходов и финансирования терроризма с учетом, как минимум, следующих специфических категорий рисков: риск по типу клиентов/контрагентов, страновой (географический) риск, риск услуги (продукта) и (или) способа ее (его) предоставления.

ТОО «EXXUS» управляет рисками информационной безопасности с указанием критериев приемлемого уровня по отношению к информационным активам.

7.16. **Общие требования к обеспечению сохранности денег клиента**

7.16.1. Способы управления рисками, применяемые в целях обеспечения сохранности денег клиента:

– осуществление расчета в пределах, предоставленных агенту/субагенту(-ам) денег;

– автоматизированное управление очередностью исполнения распоряжений Участников;

– другие способы управления рисками, предусмотренные Правилами, иными внутренними документами Товарищества.

Ответственные подразделения обязаны обеспечивать эффективное функционирование системы внутреннего контроля в рамках полномочий и ответственности, установленных внутренними документами Товарищества.

ГЛАВА 8.
ПОРЯДОК УРЕГУЛИРОВАНИЯ СПОРНЫХ СИТУАЦИЙ И РАЗРЕШЕНИЯ СПОРОВ С КЛИЕНТАМИ (ПЛАТЕЛЬЩИКАМИ)

8.1. 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.

8.2. 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: Казахстан, город Алматы, Бостандыкский район, улица Маркова, здание 61/1, почтовый индекс 050040;

2) путем личного обращения в офис платежной организации и ее нарочным предоставлением по адресу: Казахстан, город Алматы, Бостандыкский район, улица Маркова, здание 61/1, почтовый индекс 050040.

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.

8.3. 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.

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

8.5. 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.

8.6. Ответ на претензию плательщику подлежит направлению плательщику в срок, определенный п.8.4. Правил, по адресу, указанному в претензии, посредством службы доставки почтовых отправлений/корреспонденции.

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

ГЛАВА 9. ПОРЯДОК СОБЛЮДЕНИЯ МЕР ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (срок хранения информации по инцидентам, порядок по принятию неотложных мер, порядок ведения журнала учета инцидентов ИБ, порядок представления в Национальный Банк РК информации о выявленных инцидентах ИБ)

9.1 Основы обеспечения информационной безопасности Платежной организации

9.1. Основными задачами Порядка являются:

9.2. формирование унифицированного Перечня сведений о происшествиях, чрезвычайных ситуациях, инцидентах и инцидентах информационной безопасности;

9.3. определение порядка сбора, обработки, формирования и предоставления сведений о происшествиях, чрезвычайных ситуациях, инцидентах и инцидентах информационной безопасности, а также оперативного доведения информации до сведения руководства Платежной организации, в соответствии с Перечнем;

9.4. создание условий для своевременного принятия решений по предотвращению или минимизации возможного ущерба для клиента и Платежной организации;

9.5. Участники процесса информирования руководствуются нормами Законов Республики Казахстан «О противодействии терроризму», «О персональных данных и их защите», «О доступе к информации», «О национальной безопасности Республики Казахстан», «О гражданской защите», «О радиационной безопасности населения» и другие.

9.6. Порядок определяет процесс оперативного информирования о происшествиях, чрезвычайных ситуациях, инцидентах или инцидентах информационной безопасности, но не заменяет порядок оповещения государственных органов, установленный законодательством и нормативными правовыми актами Республики Казахстан.

Признаки событий информационной безопасности на объекте Платежной организации:

1) прерывание работы обслуживающих сервисов (например: электронной почты, доступа к сети интернет) продолжительностью, превышающей период обработки запросов;

2) прерывание работы оборудования (например: рабочих станций, ноутбуков, серверов сетевого оборудования и др.) продолжительностью, превышающей период обработки запросов;

3) системные сбои в работе программного обеспечения;

4) неконтролируемые изменения настроек информационных систем;

5) аномальное (отличающееся от обычно происходящих) событие информационной безопасности (например: подключение пользователя в ночное время или в период его отпуска и др.);

6) аномальная сетевая активность (например: нетипично большое количество сетевых соединений и др.);

7) аномальное поведение бизнес-приложений;

8) нарушения в процессе предоставлении доступа работникам к информационной системе;

9) получении информации о совпадении индикаторов произошедших ранее событий с индикаторами компрометации (факты соединений с определенными IP-адресами, URL-адресами).

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.

Индикаторы компрометации информации:

1. Подозрительная активность учетных записей пользователей
2. Подозрительная сетевая активность
3. Неожиданное обновление программных продуктов
4. Несанкционированное изменение конфигурационных файлов, реестров или настроек
5. Отказ функционирования прикладного ПО
6. Замедленная работа рабочей станции или сервера
7. Искажение, шифрация, дублирование или отсутствие хранимой информации
8. Большое количество неудачных попыток подключений

Платежной организацией разработан основной внутренний документ: Политика информационной безопасности ТОО «EXXUS», регламентирующий базовые понятия и положения, касающиеся формирования системы информационной безопасности. Указанный документ устанавливает основные высокоуровневые положения по обеспечению информационной безопасности, требования Политики распространяются на все информационные активы, в том числе зафиксированные на материальных носителях или передаваемые в устной или визуальной форме.

9.1.1 Порядок обеспечения информационной безопасности, процедуры по обеспечению сохранности сведений, составляющих коммерческую и служебную тайну, конфиденциальной информации, недопущение использования таких сведений, в собственных интересах (Товарищества), работников или третьих лиц содержатся в соответствующих внутренних документах Товарищества.

9.1.2 Платежная организация обеспечивает создание и функционирование системы управления информационной безопасностью, являющейся частью общей системы управления платежной организации, предназначенной для управления процессом обеспечения информационной безопасности.

9.1.3 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

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

- ✓ гарантирование использования по назначению компьютеров и телекоммуникационных ресурсов Платежной организации, ее сотрудниками, независимыми подрядчиками и другими пользователями;
- ✓ выявление, реагирование (противодействие атакам в реальном времени), разрешение и анализ причин возникновения инцидентов информационной безопасности;
- ✓ управление доступом к активам;
- ✓ антивирусная защита;
- ✓ резервное копирование данных;
- ✓ управление непрерывностью бизнеса;
- ✓ регистрация, анализ и контроль событий информационной безопасности;
- ✓ выявление уязвимостей в информационных системах платежной организации, с использованием которых могут быть реализованы угрозы информационной безопасности;
- ✓ криптографическая защита, определение требований к организации работ, эксплуатации, обеспечение сохранности и безопасное использование средств криптографической защиты.

- ✓ формирование принципов внесения изменений, процедуры установки, модификации и технического обслуживания информационных систем платежной организации;
- ✓ физическая безопасность активов;
- ✓ защита сетевого периметра;
- ✓ соблюдение условий всех программных лицензий, авторских прав и законов, касающихся интеллектуальной собственности

9.1.5 Система информационной безопасности платежной организации является совокупностью применяемых в Товариществе мер по защите информации в процессе оказания платежных услуг и осуществлении текущей деятельности.

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 конфиденциальной информации, предотвращению несанкционированного использования и защите идентификационных данных от несанкционированного доступа со стороны третьих лиц

9.2 Меры по обеспечению информационной безопасности

9.2.1 Обработка защищаемых информационных активов осуществляется сотрудниками исключительно в рамках выполнения ими должностных обязанностей. Сотрудники, должностные обязанности которых не предусматривают обработку указанной информации, не должны иметь к ней доступ.

9.2.2 При хранении материальных носителей должны соблюдаться условия, обеспечивающие сохранность таких информационных активов и исключающие несанкционированный доступ к ним.

9.2.3 Ограничения, запреты и взыскания, накладывающиеся на пользователей персональных компьютеров:

9.2.4 Сообщать, устно или письменно, кому бы то ни было (в том числе и другим сотрудникам) конфиденциальные сведения, если это не вызвано выполнением должностных обязанностей или задания руководства;

9.2.5 использовать конфиденциальные сведения в личных целях;

9.2.6 выносить из здания документы и другие носители, содержащие конфиденциальные сведения, без письменного разрешения руководителя подразделения (о чем должна быть сделана запись на данном документе);

9.2.7 снимать копии с конфиденциальных документов без письменного разрешения руководителя подразделения, в том числе используя фото-видеозапись;

9.2.8 оставлять при выходе из кабинета документы, содержащие конфиденциальные сведения на рабочих столах, а также оставлять после работы незапертыми и не опечатанными сейфы (металлические шкафы), в которых хранятся такие документы;

9.2.9 хранить конфиденциальную информацию на общих папках без разграничения доступа только для допущенных лиц;

9.2.10 передавать по незащищенным каналам связи, в том числе электронной почты, Интернет, Скайп и т.д., конфиденциальную информацию.

9.2.11 вести переговоры, содержащие конфиденциальные сведения, при поднятой телефонной трубке, включенных микрофонах.

При обработке защищаемых информационных активов их безопасность обеспечивается использованием системы защиты, включающей организационные меры и средства защиты информации (в том числе средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки таких сведений). В целях предотвращения утечки информации пользователям, в памяти компьютеров, которых находятся конфиденциальные сведения, запрещается:

работать с информацией в присутствии посторонних лиц и сотрудников Товарищества, не допущенных к этой информации;

оставлять компьютер включенным без необходимости и без блокировки экрана;

разглашать любые пароли.

Описание физической защиты информационных активов изложены во внутреннем документе Товарищества.

Требования по обработке, хранению персональных данных изложены в соответствующем внутреннем документе.

Требования к обеспечению защиты информации при оказании платежных услуг. Товарищество принимает необходимые меры для обеспечения защиты следующей информации (далее - защищаемая информация):

информация, содержащаяся в оформленных в рамках применяемой формы безналичных расчетов распоряжениях клиентов Организации;

ключевая информация средств криптографической защиты информации, используемых при совершении платежей;

информация о конфигурации, определяющей параметры работы автоматизированных систем, программного обеспечения, средств вычислительной техники, телекоммуникационного оборудования (далее - объекты информационной инфраструктуры), эксплуатация которых обеспечивается Товариществом, а также информации о конфигурации, определяющей параметры работы технических средств защиты информации;

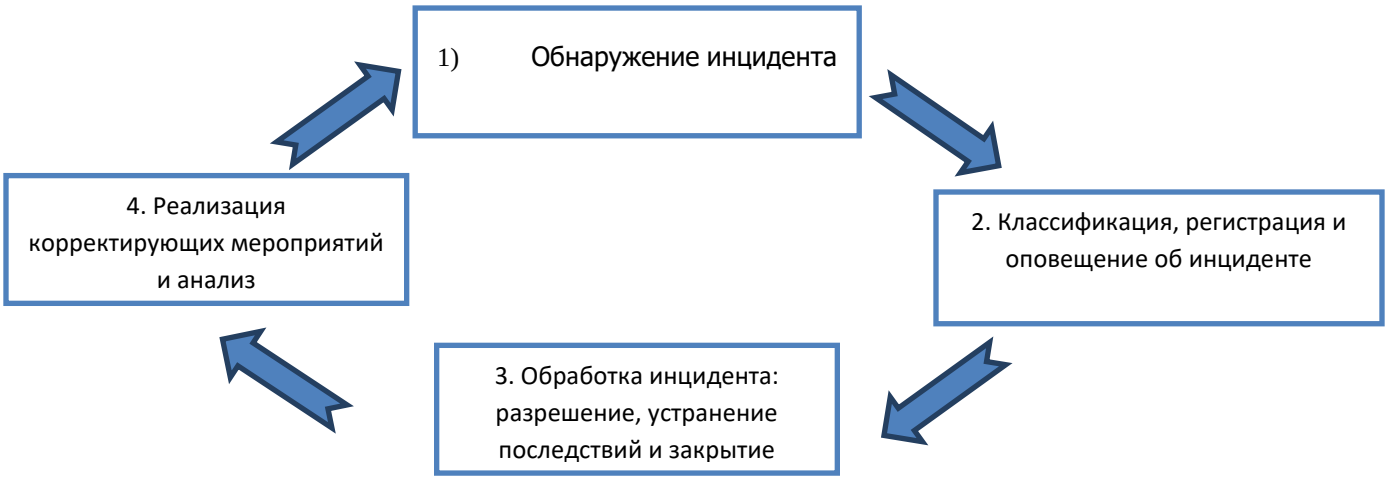
информация ограниченного доступа, в том числе персональные данные и иная информация, подлежащая обязательной защите в соответствии с законодательством Республики Казахстан.

Порядок управления инцидентами информационной безопасности

Требования данных Правил распространяются на всех работников платежной организации, а также представителей третьей стороны, связанных с платежной организацией договорными и другими обязательствами.

Жизненный цикл по управлению инцидентами ИБ

Жизненный цикл мероприятий по управлению инцидентами состоит из 4 стадий, которые следуют одна за другой и вместе составляют непрерывный цикл:



Информирование о событиях ИБ

Для предотвращения нарушений косвенно или напрямую касающихся вопросов обеспечения информационной безопасности, все работники платежной организации должны незамедлительно сообщать своему непосредственному руководителю и ответственному за разрешение инцидента обо всех обнаруженных ими событиях информационной безопасности одним из следующих способов:

1) по телефону, в том числе через сотовых операторов сети;
2) сообщением электронной почты;
3) в устной форме.

Также работник обязан информировать свое руководство и работника ответственного за информационную безопасность о любых предполагаемых недостатках в обеспечении информационной безопасности и возможностях улучшения процесса обеспечения информационной безопасности. Всем работникам, за исключением случаев, согласованных руководителем Платежной организации, запрещается предпринимать попытки использования возможных недостатков и уязвимостей в обеспечении информационной безопасности в любых целях.

В целях фиксации событий ИБ ответственный работник регистрирует инцидент ИБ в Журнале учета инцидентов информационной безопасности и ведет учет регистрации событий ИБ, а также незамедлительно сообщает руководству платежной организации.

Перечень сведений об инцидентах и инцидентах информационной безопасности

Вид сведения	Содержание	Сроки предоставления информации	Способ передачи информации
1	**2**	**3**	**4**
Инцидент/ Инцидент информационной безопасности	Сбои в работе, поломка, выход из строя или повреждение оборудования, ППП	незамедлительно	Устно по телефону Письменно специальным сообщением по электронной почте В выходные и праздничные дни устно по телефону или SMS-сообщения
	Инциденты информационной безопасности, в том числе: - утрата доступности услуг сервисов, серверного оборудования или иных устройств; - системные сбои/перегрузки рабочих станций или серверного оборудования; - несоблюдение утвержденных политик, требований и/или рекомендаций по информационной безопасности; - неконтролируемые изменения объектов информатизации; - аномальные события/поведение в системах объектов информатизации; - сбои программного обеспечения и отказы работы сервреного оборудования; - нарушение правил доступа.		
	Технические сбои либо иные инциденты, приведшие к частичной или полной недоступности информационных систем или локальной сети (отсутствие более 15 минут).		

План реагирования на кибер-инциденты

1. Работник выявивший кибер-инцидент, на основании индикаторов компрометации указанных в таблице (для выявления кибер-инцидентов), незамедлительно уведомляет об этом руководство, владельцев бизнес-процесса и ответственных администраторов;
2. Ответственные администраторы оперативно локализуют или изолируют пораженную систему;
3. В течение 24 часов Платежная организация уведомляет соответствующие внешние контролирующие стороны и каждого затронутого пользователя, в случае кибер-инцидентов ставящих под угрозу конфиденциальность, целостность или доступность их данных;
5. Устранение кибер-инцидента производится ответственными сотрудниками с возможностью привлечения сотрудников Управления киберзащиты Агентства РК;
6. После устранения кибер-инцидента производится анализ последствий кибер-инцидента, причин его возникновения для выявления и устранения уязвимостей;
7. Полностью задокументировать инцидент в соответствии с Правилами.

Порядок обработки, разрешение инцидента, устранение последствий (принятие неотложных мер)

Ответственный за разрешение инцидента и руководство платежной организации анализируют необходимую информацию с целью максимально быстрого определения того, что представляет собой инцидент ИБ, что явилось его причиной, чем или кем был вызван, на что повлиял или может повлиять, воздействие или потенциальное воздействие инцидента ИБ на сохранность, целостность и доступность информационных активов и/или деятельность платежной

организации.

Ответственный за разрешение инцидента ИБ предпринимает все меры к скорейшему разрешению инцидента ИБ. При необходимости в установленном в договорных отношениях порядке принимаются меры к привлечению представителей третьей стороны для разрешения инцидента ИБ.

В случае возникновения кибер-инцидента, в ходе реализации которого возможны нарушение штатного функционирования информационных систем, компрометации либо уничтожение данных, руководство платежной организации полностью или частично останавливают бизнес процесс, до полного устранения причин возникновения.

После разрешения инцидента ИБ ответственный за разрешение инцидента обязан заполнить отчет о закрытии инцидента в срок не более 2 (двух) рабочих дней после разрешения инцидента ИБ и согласовать отчет с администратором безопасности (если инцидент связан с информационной системой). После этого инцидент считается закрытым.

Для инцидентов информационной безопасности, вероятность возникновения которых высока и не может быть снижена в короткие сроки ответственным за разрешение инцидента в отчете дополнительно указываются методики, описывающие алгоритм обработки данного инцидента, типовые неотложные меры по локализации инцидента и его последствий.

Требования к содержанию карты инцидента, указаны в Приложении 4.

Порядок по принятию неотложных мер

На этапе реагирования на инциденты информационной безопасности ответственный за разрешение инцидента применяет стандартные процедуры реагирования, а в случаях низкой эффективности применения стандартных процедур реагирования, принимает оперативные меры реагирования на инциденты информационной безопасности, включающие следующие меры, но не ограничиваясь ими:

1) информирование и привлечение к процессу реагирования работников платежной организации, а также третьих лиц в целях обеспечения процесса эффективного противодействия инциденту информационной безопасности;

2) по согласованию с руководством платежной организации принимает ряд дополнительных мер контроля по частичной или полной остановке бизнес-процесса в платежной организации;

3) сбор данных с программно-технических средств, вовлеченных в инцидент информационной безопасности;

4) анализ инцидента информационной безопасности, его сдерживание и устранение его последствий;

5) ретроспективный анализ событий информационной безопасности на предмет выявления необработанных инцидентов информационной безопасности и (или) связанных с ними угроз информационной безопасности;

6) определение индикаторов компрометации и уязвимостей, выявленных в ходе реагирования на инциденты информационной безопасности, и реализация корректирующих мер, направленных на недопущение аналогичного инцидента информационной безопасности в дальнейшем.

Ответственный работник обеспечивает консолидацию, систематизацию, хранение, целостность и сохранность информации об инцидентах информационной безопасности в журнале учета инцидентов информационной безопасности на бумажном носителе либо в электронном виде с отражением информации об инциденте информационной безопасности, принятых мерах и предлагаемых корректирующих мерах.

Приоритеты, время реагирования и разрешения инцидентов

Приоритеты инцидентов ИБ	**Время реагирование на инциденты ИБ вне рабочего времени**	**Время реагирование на инциденты ИБ в рабочее время**	**Время разрешения инцидента ИБ**
«Очень высокий»	не более 1 часа	не более 10 минут	до 1 часа
«Высокий»	не более 4 часов	не более 20 минут	до 2 часов
«Средний»	не более 8 часов	не более 1 часа	до 6 часов
«Низкий»	Не определено	не более 2 часов	до 12 часов

Срок хранения информации о результатах внутреннего расследования инцидента информационной безопасности и материалов расследования составляет не менее 5 (пяти) лет.

Расследование инцидента ИБ

По решению руководства платежной организации расследования инцидентов ИБ проводятся комиссией, которая создается из числа представителей платежной организации и заинтересованных третьих сторон. Основной целью расследования инцидента ИБ является раскрытие всех причинно-следственных связей и получение исчерпывающей информации касаемо каждого инцидента ИБ в отдельности.

Анализ и реализация корректирующих мероприятий

В ходе обработки инцидента ИБ ответственный за разрешение инцидента производит анализ инцидента, принимает необходимые меры по недопущению повтора инцидента ИБ и вносит предложения о недопущении повторения (предложения по улучшению) в Отчет о разрешении инцидентов.

Отчеты о разрешении инцидентов консолидируются в сводный отчет и выносятся на рассмотрение руководства платежной организации для выработки корректирующих мероприятий с учетом рисков их повторного возникновения.

Порядок ведения журнала учета инцидентов информационной безопасности

Платежная организация в целях регистрации учета инцидентов ИБ осуществляет ведение журнала, с указанием информации при регистрации событий информационной безопасности:

1. номер п/п;
2. дата/время регистрации события;
3. ФИО, организация, подразделение, должность сотрудника, сообщившего о событии, наименование ИС;
4. описание события (место, время обнаружения, ИС, возможные причины);
5. приоритет инцидента ИБ;
6. ФИО ответственного за обработку инцидента ИБ.

Журнал регистрации инцидентов информационной безопасности пронумеровывается, прошнуровывается, сшивается и удостоверяется подписью лица, ответственного за разрешение инцидента. Ошибочные записи в журнале регистрации, подлежащие корректировке, также удостоверяются подписью данного лица.

Порядок представления в Национальный Банк РК информации о выявленных инцидентах информационной безопасности

После действий, описанных в разделе настоящих правил «Информирование о событиях ИБ» ответственный за разрешение инцидента незамедлительно представляет информацию (по всем доступным каналам связи и письменно) об инцидентах информационной безопасности, зарегистрированной в платежной организации в соответствии с главой 6 Правил 215, а также по форме согласно приложению 7 к Правилам 215.

После разрешения и исправления инцидента ИБ, ответственный за разрешение инцидента по согласованию с руководством платежной организации направляет через платформу Национального Банка для обмена событиями и инцидентами информационной безопасности информацию по обработанным инцидентам платежной организации.

ГЛАВА 10. ОПИСАНИЕ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ И ОБОРУДОВАНИЯ, НЕОБХОДИМЫХ ДЛЯ ОКАЗАНИЯ ПЛАТЕЖНЫХ УСЛУГ

10.1. Основу технического обеспечения информационных технологий составляют оборудование, программное обеспечение, являющиеся ядром любой информационной системы. Товариществом разработан и утвержден внутренний документ: Положение о программно-техническом обеспечении ТОО «EXXUS» и иные внутренние документы, содержащие описание информационных и технологических средств и систем безопасности, общее описание программно-технического обеспечения, используемого ТОО «EXXUS» при осуществлении текущей деятельности, а также механизмы и системы контроля, применяемые Платежной организацией при оказании платежных услуг, и другие положения.

10.2. Платежная организация в целях оказания платежных услуг, а также для ведения внутреннего учета и автоматизации процессов внутреннего контроля в том числе в целях противодействия отмыванию доходов, полученных незаконным путем и финансированию терроризма, в соответствии с учетной регистрацией Национального Банка РК использует программное обеспечение:

1) Программное обеспечение, используемое при оказании платежных услуг по приему наличных денег для осуществления платежа без открытия банковского счета отправителя денег, обеспечивает прием наличных денег от плательщика, внесенных через электронные терминалы (устройства), принадлежащие платежным агентам/субагентам, и последующего осуществления платежа без открытия банковского счета в пользу получателя. Описание программно-технических средств и оборудования, необходимых для оказания указанных платежных услуг содержится в Приложении № 2 и 3 к настоящим Правилам.

2) В целях оказания платежных услуг по обработке платежей, инициированных клиентом в электронной форме, и передаче необходимой информации банку, филиалу банка-нерезидента Республики Казахстан, организации, осуществляющей отдельные виды банковских операций, для осуществления платежа и (или) перевода либо принятия денег по данным платежам, Товарищество использует 2 вида программного обеспечения:

- программное обеспечение, позволяющие мерчанту при помощи интернет-ресурсов принимать в качестве оплаты за товары и услуги банковские карточки;

- программное обеспечение Система по учету платежей в качестве учетной системы для регистрации распоряжений плательщиков на осуществление платежа, которое обеспечивает автоматизацию агрегирования, проведения платежей по разного рода услуг и сервисов, учет оборотов, планирование оборотов, предоставляющая доступ по протоколу API различным операторам услуг.

10.3. Основные требования защиты информации, хранящейся на персональных компьютерах и систем:

Персональные компьютеры (ноутбуки) пользователей должны быть физически защищены от вскрытия, должны быть приняты меры для обнаружения и обезвреживания злонамеренных программ (компьютерные вирусы, сетевые черви, «троянские кони», логические бомбы), а также приняты меры защиты от несанкционированного доступа в отсутствии пользователя.

Физическая защита должна включать в себя мероприятия, предотвращающие несанкционированное вскрытие персональных компьютеров с целью получения доступа к носителям информации, находящимся в корпусе системного блока, а также для изменения конфигурации компьютера и настроек BIOS.

Защита персонального компьютера пользователя от утечки конфиденциальной информации по информационным каналам должна включать в себя мероприятия, направленные на разграничение доступа по сети к информационным ресурсам компьютера авторизованных пользователей и ограничение доступа для неавторизованных пользователей, а также предотвращение занесения и распространения злонамеренных программ.

Защита доступа к персональному компьютеру должна включать в себя мероприятия, препятствующие несанкционированному доступ к компьютеру пользователя в его отсутствие.

Работа пользователей в ОС и ИС осуществляется под уникальными учетными 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 Компании (для лиц, не являющихся работниками Компании, для работников, которым необходимо получить временный доступ к ресурсам Компании, и т.п.) необходимо использовать временные учетные записи (с фиксированным сроком действия) в ОС.

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 Компании 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 Компании, 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».

Программно-технические меры по обеспечению информационной безопасности платежной организации включают в себя систему:

1) управления доступом;
2) протоколирования и проверки технического состояния;
3) криптографической защиты данных.

Система управления доступом обеспечивает выполнение следующих мероприятий:

a) определение перечня групп данных, задач и установления им уровня секретности;
b) установление способов и процедур защиты каждой группы данных;
c) определение групп пользователей информационных систем и разбиение их на категории по выполняемым функциям и установление им уровней доступа к информации;
d) установление порядка идентификации категории пользователей;
e) идентификация и аутентификация пользователей при входе в систему по специальным устройствам (электронным ключам) и паролю временного действия длиной не менее шести буквенно-цифровых символов;
f) аппаратная идентификация и аутентификация терминалов, персональных компьютеров, узлов компьютерной сети, каналов связи, внешних устройств вычислительных машин по уникальным встроенным устройствам;

С момента установления пользователям, группе пользователей, обслуживающему персоналу прав доступа к ресурсам информационной системы программно-техническим средствами системы ведется протоколирование, сбор и накопление информации о происходящих в системе событиях.

В процессе протоколирования событий системы записывается следующая информация:

1) дата и время события;
2) идентификатор инициатора события;
3) тип события;
4) результат действия (успех или неудача);
5) источник запроса (имя терминала);
6) имена затронутых объектов (открываемых, копируемых или удаляемых файлов);
7) описание изменений, внесенных в базы данных защиты (новая метка безопасности объекта);

10.3. В программном обеспечении (независимо от уровня доступа) не допускается:

✓ содержание средств, позволяющих исполнить определенные функции и операции с нарушением установленного порядка их выполнения;

✓ иметь функции, позволяющие напрямую вносить изменения в данные сформированных выходных документов;

✓ изменение/удаление данных о проведенных операциях и о состоянии лицевых счетов, за исключением специально предназначенных для этого операций (функций);

✓ дополнительные требования устанавливаются соответствующим внутренним документом Товарищества.

10.4. Требования Платежной организации к информационным и технологическим средствам, используемым для оказания платежных услуг

п/п	Требование	Описание требований
	Основные требования, предъявляемые к серверам	1) надежность; 2) производительность; 3) управляемость; 4) расширяемость (масштабируемость).
	Основные требования к техническому обеспечению (оснащению) серверов	1) Процессор 4 ядра (8 логических потоков), частота – 3-3,5 ГГц и больше 2) Оперативная память 64 Гб и больше

		3) Свободное дисковое пространство 256 Гб (зависит от размера хранимых в системе документов) 4) Пропускная способность сетевого интерфейса 1 Гбит/с
	Основные требования к системному (программному) обеспечению серверов	1) прозрачность работы 2) гарантированная надежность выполнения в соответствии со спецификациями (спецификациями называются функциональные требования) 3) максимальная скорость выполнения 4) минимальные затраты на хранение машинных кодов 5) поддержка стандартных средств связи с прикладными программами
.1.	Система хранения данных	SSD 300 ГБ и больше
.2.	База данных	Не ниже MSSQL Server 2016
.3.	Система резервного копирования	Synology NAS, Hyper Backup Vault
.4.	Антивирусная защита	Symantec Endpoint Protection
	Основные требования к Системе (программному обеспечению), используемому для оказания Платежных услуг	1) Обеспечение информационного и технологического взаимодействия между участниками расчетов при оказании платежных услуг в соответствии с механизмами и требованиями законодательства Республики Казахстан. 2) Совместимость Системы с ОС, установленной на Серверах. 3) Ежедневное резервное копирование информации и данных, хранящихся в Системе. 4) Протоколирование всех событий и действий, совершаемых посредством Системы. 5) Наличие функции по ограничению доступа к Системе в соответствии с ролями пользователей. 6) Наличие модуля по ведению аналитического учета проводимых операций, выгрузка аналитической и статистической информации по оказанным Платежным услугам из Системы. 7) Возможность передачи данных банкам-партнерам о проводимых операциях в виде XML-файлов. 8) Гибкость Системы на доработку в соответствии с требованиями бизнеса и законодательства Республики Казахстан. 9) Возможность интеграция со сторонними системами с использованием протокола безопасной передачи данных (SSL).

10.5. Организация бесперебойной работы оборудования

Для предотвращения потерь информации при кратковременном отключении электроэнергии все ключевые элементы, сетевое и коммуникационное оборудование, а также наиболее критичные рабочие станции должны подключаться к сети электропитания через источники бесперебойного питания. В зависимости от необходимого времени работы ресурсов после потери питания могут применяться следующие методы резервного электропитания:

✓ локальные источники бесперебойного электропитания с различным временем питания для защиты отдельных компьютеров;

- ✓ источники бесперебойного питания с дополнительной функцией защиты от скачков напряжения;
- ✓ резервные линии электропитания в пределах комплекса зданий;
- ✓ аварийные электрогенераторы.
- ✓ Системы обеспечения отказоустойчивости:
- ✓ технология RAID. Для защиты от отказов отдельных дисков серверов, осуществляющих обработку и хранение защищаемой информации, должны использоваться технологии RAID, которые (кроме RAID-0) применяют дублирование данных, хранимых на дисках.

- ✓ Система резервного копирования и хранения данных, должна обеспечивать хранение защищаемой информации на надежный носитель (жесткий диск и т.п.).

10.6. Руководством Платежной организации обеспечивается установление уровней доступа для каждого пользователя программного обеспечения, а также вход по индивидуальному паролю. В программном обеспечении не должно быть возможности доступа к входным данным, функциям, операциям, отчетам без ввода соответствующего пароля.

10.7. Защита информации должна обеспечиваться следующими основными функциями уровня доступа «администратор»:

- ✓ определение групп пользователей, разделение их на категории по выполняемым функциям и установление им уровней доступа к информации, смена паролей;

- ✓ блокирование доступа пользователей к данным и функциям программного обеспечения;
- ✓ настройка параметров функционирования программного обеспечения;
- ✓ просмотр подключенных к базе данных программного обеспечения пользователей;
- ✓ отключение пользователей от базы данных программного обеспечения в случае необходимости;
- ✓ смена рабочей даты;
- ✓ создание архивных и резервных копий на съемных носителях данных долговременного хранения.

10.8. Основными функциями уровня доступа "пользователь" являются:

- ✓ смена пользователем собственного пароля;
- ✓ периодическое обновление справочной информации в базе данных программного обеспечения;
- ✓ ввод данных в программное обеспечение;
- ✓ проведение в программном обеспечении определенных операций;
- ✓ формирование отчетных/выходных форм;
- ✓ сохранение необходимой информации;
- ✓ печать отчетов и выходных документов.

10.9. В программном обеспечении (независимо от уровня доступа) не допускается:

- ✓ содержание средств, позволяющих исполнить определенные функции и операции с нарушением установленного порядка их выполнения;
- ✓ иметь функции, позволяющие напрямую вносить изменения в данные сформированных выходных документов;
- ✓ изменение/удаление данных о проведенных операциях и о состоянии лицевых счетов, за исключением специально предназначенных для этого операций (функций).

10.10. Порядок доступа к ресурсам (дисковое пространство, директории, сетевые ресурсы, базы данных и другие), выделенным для накопления в них информации для передачи в информационную среду с использованием системы защиты, получения информации из информационной среды, хранения, архивирования либо другой обработки информации, должен исключать возможность несанкционированного доступа к этим ресурсам.

10.11. Платежной организацией разработан и утвержден внутренний документ: Политика управления доступом, регистрацией и парольной защитой, иные внутренние документы, регламентирующие требования к программно-техническим, оборудованию, порядку их использования, уровням доступа, обеспечения физической защиты и т.д.

10.12. **Справка о составе технических средств, обеспечивающих процесс оказания платежных услуг**

Комплекс технических средств Системы включает средства обработки данных (ПЭВМ, сервера БД, комплекс ПО по обработке данных БД), средства обмена данными в ЛВС с возможностью выхода в глобальные сети (кабельная система, коммутаторы, маршрутизаторы и т.д.), а также средства хранения (в т.ч. архивирования) данных.

К основным особенностям функционирования Системы, относятся:

- ✓ объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- ✓ большое разнообразие решаемых задач и типов обрабатываемых сведений (данных), сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей;
- ✓ объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;
- ✓ непосредственный доступ к вычислительным и информационным ресурсам большого числа различных категорий пользователей (источников и потребителей информации)
- ✓ наличие большого числа каналов взаимодействия с “внешним миром” (источниками и потребителями информации);
- ✓ непрерывность функционирования Системы;
- ✓ высокая интенсивность информационных потоков в Системе;
- ✓ наличие в Системе ярко выраженных функциональных систем (ИС), с различными требованиями по уровням защищенности (физически объединенных в единую сеть);
- ✓ разнообразие категорий пользователей и обслуживающего персонала системы.

В качестве каналов связи используется интернет-соединение используя криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет**.**

ГЛАВА 11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Изменения и дополнения в настоящие Правила могут быть внесены путем принятия соответствующего решения общим собранием участников (если Уставом Товарищества полномочие по утверждению/принятию внутренних документов не отнесено к компетенции исполнительного органа) об утверждении изменений и/или дополнений в Правила, в том утверждение внутреннего документа в новой редакции.

11.2. Все, что не урегулировано настоящими Правилами и другими внутренними документами Платежной организации, регулируется положениями договоров с контрагентами и(или) нормами действующего законодательства Республики Казахстан.

11.3. Требования настоящих Правил обязательны для исполнения всеми работниками Платежной организации. За неисполнение и ненадлежащее исполнение требований настоящих Правил работники Товарищества несут ответственность в соответствии с законодательством Республики Казахстан и внутренними нормативными документами Платежной организации.

11.4. В случае если отдельные нормы настоящих Правил вступят в противоречие с законодательством Республики Казахстан, они утрачивают силу и применяются соответствующие нормы законодательства Республики Казахстан. Недействительность отдельных норм настоящих Правил не влечет недействительности других норм и Правил в целом

Список Приложений к настоящим Правилам

№	Приложение	Наименование
1	**Приложение № 1**	Тарифы Платежной организации при оказании платежных услуг по приему наличных денег для осуществления платежа без открытия банковского счета
2	**Приложение № 2, 3**	Техническая характеристика терминалов, POS терминалов и иных технических средств
3	**Приложение № 4**	Карта инцидентов

Приложение № 1
к Правилам осуществления деятельности платежной организации ТОО «EXXUS»

СТОИМОСТЬ УСЛУГ ПО ПРИЕМУ НАЛИЧНЫХ ДЕНЕГ ДЛЯ ОСУЩЕСТВЛЕНИЯ ПЛАТЕЖА БЕЗ ОТКРЫТИЯ БАНКОВСКОГО СЧЕТА ОТПРАВИТЕЛЯ ДЕНЕГ

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

Приложение № 2
к Правилам осуществления деятельности платежной организации ТОО «EXXUS»

Техническая характеристика терминалов, POS терминалов и иных технических средств

Терминалы самообслуживания

Корпус	**Напольный, одномониторный, для помещений**
Цвет	**Любой по RAL**
Мониторная сборка	**Монитор: ЖК 17"** **Сенсорное стекло: GeneralTouch 17" вандалостойкое, 6мм**
Компьютерные комплектующие	**Материнская плата: GIGABYTE / ASUS, H81, Soc 1150** **Блок питания: FSP 350PNR** **Процессор: INTEL Celeron G1820, LGA 1150** **Жесткий диск: 2.5" HHD 320Gb** **Модуль памяти: DDR3 - 2Гб, 1666** **Контроллер: PCI 2 COM (9835)** **Устройство охлаждения: Socket 1150**
Блок питания термопринтера	**24V, 150W, 6.25A**
Купюроприемник	**CashCode MVU-1024 (СЦ) с прошивкой VU-KZ1313**
Инкассаторский мешок	**2500 купюр**
Термопринтер	**Custom TG2480H (СЦ)**
GPRS-модем	**Siemens MC35i**
Антенна	**GPRS внешняя**
Монетоприемник	**NRI G13mft.18U (USB)**
Сторожевой таймер	

Примечание*
Комплектующие материалы в аппарате могут быть изменены

Приложение № 3
к Правилам осуществления деятельности платежной организации ТОО «EXXUS»

Техническая характеристика терминалов, POS терминалов и иных технических средств

Технические характеристики PAX-S/P 90; Lipman Nurit 8010 (Verifone); Visiontek 92-92G

Процессор: 32-bit RISC, 200MHz **Объём памяти**: 4 Mb FLASH, 8 Mb SDRAM **Принтер:** термический, бумага 58мм, рулон 38мм, скорость 12,5 линий/сек **Экран LCD:** 128x64 с подсветкой **Клавиатура:** 10 алфавитно-цифровых клавиш, 9 функциональных клавиш, тумблер питания **Считыватель магнитной полосы:** ISO7812, Track 1/2/3, чтение в любом направлении **Считыватель чип-карт:** 1 для карты клиента (EMV2000) 1 для карты продавца (ISO7816) **PSAM слоты:** 2 ISO7816 **Устройство связи:** GPRS, CDMA **Периферийные порты:** 1 RS232, 1 зарадка батареи, 1 телефон **Питание (внешний адаптер) Вход:** AC110-220V, 50, 60Hz,1.0A**;** **Выход:** 9.5V (2.0A), DC 4.2V (4.0A**)** **Батарейка литий-ионная:** 180 мАч, 7.4В, не менее 24 часов работы или 200 транзакций **Условия эксплуатации:** to 0~ +50C, влажность 10%-95% **Условия хранения:** to -20C ~ +60C, влажность 5%~95% **Размеры, мм:** 205 x 89,5 x 53 mm **Вес, г**: 481 г	**Графический дисплей** 128x128 с подсветкой и touchscreen'ом; **Считыватель магнитных карт**; **Мощный процессор ARM 7**; 2 Мб RAM; 4 Мб флеш-памяти для хранения приложений; 2 SAM модуля с доступом; **Радиомодем** (GSM&GPRS(с возможностью подключения гарнитуры для голосовой связи), CDMA, CDPD, Mobitex, DataTac); **Телефонный модем** 33600 бит/сек; поддержка TCP/IP; **Встроенная пин-клавиатура** с поддержкой DES, 3DES, MAC, RSA; **Термопринтер** 12 строк/сек; **Вес** - 600 г.
	Visiontek 92 Процессор и память: 32-bit ARM Core CPU 70MHz 8 MB флеш-памяти 16MB ОЗУ Синхронный или асинхронный канал TCP/IP GSM, GPRS (двухдиапазонный) Вес 750 г

Приложение № 4
к Правилам осуществления деятельности платежной организации ТОО «EXXUS»

Карта инцидента информационной безопасности

№	Общие сведения	
	Характеристики инцидента информационной безопасности	Информация об инциденте информационной безопасности
1	Наименование инцидента информационной безопасности	
2	Дата и время выявления (дд.мм.гггг и чч:мм с указанием часового пояса UTC+X)	
3	Место выявления (организация, филиал, сегмент информационной инфраструктуры)	
4	Источник информации об инциденте информационной безопасности (пользователь, администратор, администратор информационной безопасности, работник подразделения информационной безопасности или техническое средство)	
5	Использованные методы при реализации инцидента информационной безопасности (социальная инженерия, внедрение вредоносного кода)	
Содержание инцидента информационной безопасности		
6	Симптомы, признаки инцидента информационной безопасности	
7	Основные события (эксплуатация уязвимостей в прикладном и системном программном обеспечении; несанкционированный доступ в информационную систему; атака «отказ в обслуживании» на информационную систему или сеть передачи данных; заражение сервера вредоносной программой или кодом; совершение несанкционированного перевода денежных средств; инциденты информационной безопасности, несущие угрозу стабильности деятельности платежной организации)	
8	Пораженные активы (физический уровень информационной инфраструктуры, уровень сетевого оборудования, уровень сетевых приложений и сервисов, уровень операционных систем, уровень технологических процессов и приложений и уровень бизнес-процессов платежной организации)	
9	Статус инцидента информационной безопасности (свершившийся инцидент информационной безопасности, попытка осуществления инцидента информационной безопасности, подозрение на инцидент информационной безопасности)	
10	Ущерб	

11	Источник угрозы (выявленные идентификаторы)	
12	Преднамеренность (намеренный, ошибочный)	
Предпринятые меры по инциденту информационной безопасности		
13	Предпринятые действия (идентификация уязвимости, блокирование, восстановление)	
14	Запланированные действия, направленные на минимизацию возникновения рисков информационной безопасности	
15	Оповещенные лица (фамилия, имя, отчество (при его наличии) должностных лиц, наименование государственных органов, организаций)	
16	Привлеченные специалисты (фамилия, имя, отчество (при его наличии) место работы, должность, номер телефона)	

Ответственный работник по информационной безопасности

_____ _____

(фамилия, имя, отчество (при его наличии) (подпись)

Дата «____» _____ 20 ___ года