Общество
с ограниченной
ответственностью
«Единый
общереспубликанский
процессинговый центр»

«УТВЕРЖДЕНО»
Генеральным директором
ООО «Единый общереспубликанский
процессинговый центр»

# РЕГЛАМЕНТ ПРОВЕДЕНИЯ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКОЙ ПРОВЕРКИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПЛАТЕЖНОЙ СИСТЕМЫ UZCARD

ТАШКЕНТ - 2024

Оглавление

**Перечень используемых сокращений**

| | |
|---|---|
| **Партнер** | Поставщики платежных услуг (банк, платежная организация, платежный агент и платежный субагент) |
| **ИБ** | Информационная безопасность |
| **ОТП** | Организационно-техническая проверка Партнера |
| **ТИБ** | Требования информационной безопасности, изложенные в Правилах ПС «UZCARD» |
| **ПС «UZCARD»** | Платежная система «UZCARD», деятельность по обеспечению функционирования которой осуществляется со стороны Оператора |
| **ИСП** | Информационная система Партнера, состоящая из комплекса специализированных компьютерных программных продуктов, функционирование которой обеспечивается путем информационного и технологического взаимодействия Партнера и Оператора, предназначенное для создания дополнительного сервиса, обеспечения информационной поддержки и других услуг, оказываемых Партнером своим клиентам. |
| **ПО «SV-Gate»** | Программное обеспечение Оператора, предназначенное для технологического взаимодействия ИСП с ПС «UZCARD» и позволяющее пользоваться услугами Оператора через ИСП |
| **Оператор** | ООО «Единый общереспубликанский процессинговый центр» |
| **Договор** | Договор, заключенный между Оператором и Партнером во временное возмездное пользование учетные записи и права пользования ПО «SV-Gate» посредством API (простая неисключительная лицензия). |
| **Партнер** | Банк, платежная организация, платежный агент, платежный субагент с которым заключен Договор. |
| **КД** | Коммерческий департамент Оператора. |
| **ТКО** | Постоянно действующая Техническая комиссия Оператора по организации и проведения ОТП. |

## 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящий документ определяет порядок ОТП на соответствие требованиям информационной безопасности ПС «UZCARD», который осуществляет ООО «ЕОПЦ» (далее - Оператор) на условиях, установленных настоящим Регламентом, ТИБ и Договором.

1.2. Целью проведения ОТП является оценка готовности организационных и технических средств Партнера в области ИБ в ИСП, состоящая из комплекса специализированных компьютерных программных продуктов (далее – ИСП), подключаемой либо уже подключенной к ПО «SV-Gate».

1.3. Перечень документов, на основании которых проводится ОТП:

- Закон Республики Узбекистан №578 от 01.11.2019 «О платежах и платежных системах»;
- Правила ПС «UZCARD»;
- Договор;

1.4. Участники проведения ОТП:

- Партнер;
- КД;
- ТКО.

## 2. ТИПЫ ПРОВЕДЕНИЯ ОТП

2.1. ОТП проводится на основании заключенного Договора между Оператором и Партнером на регистрацию учетной записи и предоставление права пользования ПО «SV-Gate».

2.2. ОТП разделяется на 3 (три) типа:

**2.2.1. Первичная ОТП** – схема проведения предоставлена в Приложении 3;

**2.2.2. Вторичная ОТП** – схема проведения предоставлена в Приложении 4;

**2.2.3. ОТП по форме самостоятельной оценки** – схема проведения предоставлена в Приложении 5.

## 3. ПЕРВИЧНАЯ ОТП

*3.1. Общий порядок*

Первичная ОТП проводится при первоначальном подключении Партнера к ПО «SV-Gate». При этом подразумевается, что Партнер не имеет доступа к ПО «SV-Gate» и намеревается подключить свою информационную систему к ПО «SV-Gate». Основанием для проведения ОТП является Договор.

*3.2. Предварительное ознакомление Партнера с ТИБ и настоящим Регламентом*

После заключения Договора КД проводит ознакомление Партнера с ТИБ и настоящим документом путем передачи интернет-ссылок на настоящий Регламент и ТИБ. После ознакомления с вышеуказанными документами Партнер начинает процесс подготовки пакета требуемых данных, указанных в ТИБ.

*3.3. Планирование ОТП*

На этапе планирования ТКО проводит процесс согласования проведения ОТП с Партнером. Первичная ОТП проводится с выездом представителей ТКО на территорию Партнера. При отсутствии возможности выезда представителей ТКО по операционным причинам формат проведения ОТП может быть изменен на онлайн формат с предварительным согласованием ТКО и Партнера.

*3.4. Проведение ОТП*

На данном этапе Партнер предоставляет данные ТКО, на основе которых проводится основной этап ОТП, где производится анализ предоставленных данных на соответствие

ТИБ. Детальное описание проведения ОТП приведен в *Приложении 1*.

*3.5. Итоговый отчет и оценка соответствия*

После проведения ОТП ТКО начинает подготовку итогового отчета. При выявлении несоответствий происходит процесс взаимодействия с Партнером по устранению выявленных несоответствий. На основе полученных данных ТКО завершает отчет и дает оценку готовности ИСП на соответствие ТИБ:

a) ИСП соответствует ТИБ, активация учетной записи Партнера одобряется;
b) ИСП частично соответствует ТИБ, активация учетной записи Партнера одобряется с условным периодом до 90 календарных дней;
c) ИСП не соответствует ТИБ, активация учетной записи Партнера не одобряется.

В случае если ИСП не соответствует ТИБ, активация учетной записи по доступу к ПО «SV-Gate» не производится. КД направляет отчет Партнеру и назначается повторная техническая проверка. Повторная техническая проверка ИСП осуществляется не ранее 90 (девяноста) календарных дней с даты выдачи отрицательного отчета, если сторонами не согласован более ранний срок. Если со стороны Партнера не было предоставлено свидетельство устранения несоответствий, КД инициирует процедуру расторжения договора.

## 4. ВТОРИЧНАЯ ОТП

*4.1. Общий порядок*

Вторичная ОТП Партнера применяется к Партнерам, уже имеющие доступ к ПО «SV-Gate». Вторичная ОТП Партнеров проводится согласно внутреннему «Плану проведения ОТП Партнеров», разработанную ТКО и КД.

*4.2. Оповещение Партнера*

Вторичная ОТП Партнера проводится на основании письма уведомления о предстоящей ОТП. После составления внутреннего «Плана проведения ОТП Партнеров» совместно ТКО и КД начинается процесс подготовки и отправки письма уведомления Партнеру о предстоящей ОТП за 30 (тридцать) календарных дней до начала Вторичной ОТП. Партнер, после получения письма, в течение 3 (трех) рабочих дней подтверждает получение уведомления и начинает подготовку к Вторичной ОТП.

*4.3. Планирование Вторичной ОТП*

ТКО проводит процесс согласования проведения ОТП с Партнером, согласно процессу, описанного в *Приложении 1*. Вторичная ОТП проводится с выездом представителей ТКО на территорию Партнера. При отсутствии возможности выезда представителей ТКО по операционным причинам формат проведения ОТП может быть изменен на онлайн формат с предварительным согласованием ТКО и Партнера.

*4.4. Проведение Вторичной ОТП*

На данном этапе Партнер предоставляет данные ТКО, на основе которых проводится основной этап ОТП, где производится анализ предоставленных данных на соответствие ТИБ. Детальное описание проведения ОТП приведен в *Приложении 1*.

*4.5. Итоговый отчет и оценка соответствия*

После проведения ОТП ТКО начинает подготовку итогового отчета. При выявлении несоответствий происходит процесс взаимодействия с Партнером по устранению выявленных несоответствий. На основе полученных данных ТКО завершает отчет и дает оценку готовности ИСП на соответствие ТИБ:

a) ИСП соответствует ТИБ, дальнейшее использование учетной записи Партнера

одобряется;

b) ИСП частично соответствует ТИБ, дальнейшее использование учетной записи Партнера одобряется с условным периодом до 90 календарных дней;
c) ИСП не соответствует ТИБ, дальнейшее использование учетной записи Партнера не одобряется.

В случае если ИСП не соответствует ТИБ, учетная запись по доступу к ПО «SV-Gate» ограничивается либо учетная запись отключается. КД направляет отчет Партнеру и назначается повторная техническая проверка. Повторная техническая проверка ИСП осуществляется не ранее 90 (девяноста) календарных дней с даты выдачи отрицательного отчета, если сторонами не согласован более ранний срок. Если со стороны Партнера не было предоставлено свидетельств устранения несоответствий, УКД инициирует процедуру расторжения договора.

## 5. ОТП ПО ФОРМЕ САМОСТОЯТЕЛЬНОЙ ОЦЕНКИ

*5.1. Общий порядок*

Заполнение формы самостоятельной оценки на ТИБ (далее - Форма) запрашивается Партнером не реже 1 (одного) раза в год. Решение о проведении оценки путем заполнения Формы принимается исключительно ТКО в ходе составления внутреннего «Плана проведения ОТП Партнеров».

*5.2. Оповещение Партнера*

КД начинает процесс подготовки и рассылки письма уведомления Партнеру о предстоящей ОТП, с приложением ссылки на Форму.

Партнер, после получения письма в течение 3 (трех) рабочих дней подтверждает и начинает процесс заполнения Формы. При появлении вопросов Партнер может обратиться к ТКО для уточнений и дополнений. После заполнения Формы Партнер направляет официальное письмо Оператору с приложением заполненной Формы.

ТКО получает заполненную Форму и проводит анализ полученных в ней данных.

*5.3. Итоговый отчет и оценка соответствия*

После анализа полученных данных ТКО начинает подготовку итогового отчета. При выявлении несоответствий происходит процесс взаимодействия с Партнером по устранению выявленных несоответствий. На основе полученных данных ТКО завершает отчет и дает оценку готовности ИСП на соответствие ТИБ:

a) ИСП соответствует ТИБ, дальнейшее использование учетной записи Партнера одобряется;
b) ИСП частично соответствует ТИБ, дальнейшее использование учетной записи Партнера одобряется с условным периодом до 90 календарных дней;
c) ИСП не соответствует ТИБ, дальнейшее использование учетной записи Партнера не одобряется.

В случае если ИСП не соответствует ТИБ, учетная запись по доступу к ПО «SV-Gate» ограничивается либо учетная запись отключается. КД направляет отчет Партнеру и назначается повторная техническая проверка. Повторная техническая проверка ИСП осуществляется не ранее 90 (девяноста) календарных дней с даты выдачи отрицательного отчета, если сторонами не согласован более ранний срок. Если со стороны Партнера не

было предоставлено свидетельств устранения несоответствий, УКД инициирует процедуру расторжения договора.

## 6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

6.1. Настоящий регламент вступает в силу с даты, указанной в соответствующем приказе о вступлении в силу документа.

6.2. Ответственные лица за исполнение настоящего регламента сотрудники Департамента обеспечения информационной безопасности согласно вышеуказанному приказу.

6.3. Настоящий регламент может пересматриваться при изменении нормативно-правовых актов Республики Узбекистан, нормативных актов и предписаний, регулирующих и надзорных органов, договорных условий Компании со сторонними организациями, результатов аудита по информационной безопасности, а также по инициативе генерального директора, заместителя генерального директора по техническим вопросам, директора департамента обеспечения информационной безопасности.

**Приложение 1**
к «Регламент проведения организационно-технической проверки на соответствие требованиям информационной безопасности платежной системы UZCARD»

## ДЕТАЛЬНЫЙ ПРОЦЕСС ПРОВЕДЕНИЯ ОТП

*1. Предварительный сбор информации для подготовки к ОТП.*

Для предварительного сбора информации ТКО направляется Партнеру документ «Исходные сведения», приведенный в Приложении 2 для заполнения со стороны Партнера.

При заполнении документа «Исходные сведения» со стороны Партнера предоставляется следующая информация:

- Сведения о Партнере: организационно-правовая форма и фирменное наименование Партнера, исполнительный орган (наименование должности и ФИО), руководитель проекта ИСП (наименование должности и ФИО), системный администратор ИСП (наименование должности и ФИО), ответственный по вопросам ИБ ИСП (наименование должности и ФИО).
- Программные средства ИСП.
- Сетевые технические средства ИСП.
- Места хранения данных банковских карт ИСП.
- Организационно-распорядительные документы в области ИБ Партнера.

*2. Определение области ОТП*

На данном этапе определяется область проведения ОТП, т.е. область применения документа ТИБ. Основной областью проведения ОТП является сегмент работы ИСП, взаимодействующий с ПО «SV-Gate». В сегмент работы ИСП входит:

- Нормативно-распорядительные документы, определяющие работу ИБ.
- Сервер приложения ИСП – виртуальный сервер, где обрабатываются данные банковских карт, полученные с ПО «SV-Gate». Количество серверов приложения может быть более одного виртуального сервера, при развертывании структуры с учетом отказоустойчивости и распределения нагрузки (Load balancing).
- Сервер СУБД ИСП – виртуальный сервер, где настроена база данных ИСП и обеспечивает хранение и обработку данных банковских карт, полученные с ПО «SV-Gate». Количество серверов приложения может быть более одного виртуального сервера, при развертывании структуры с учетом отказоустойчивости и распределения нагрузки (Load balancing).
- Сервер балансировщика нагрузки – виртуальный сервер, который играет роль распределения нагрузки и/или является отдельным сервером, взаимодействующий с ПО «SV-Gate» и сервером ИСП.
- Межсетевые экраны, взаимодействующие с ПО «SV-Gate» и контролирующие сегмент ИСП на сетевом уровне. Модули обнаружения и предотвращения сетевых вторжений на сегмент ИСП, входящие в состав межсетевых экранов, также входят в область применения ОТП.
- Средства обеспечения ИБ, взаимодействующие с сегментом ИСП, такие как:
  - Система сбора и корреляции событий (SIEM);
  - Система управления привилегированным доступом (PAM);
  - Система антивирусной защиты (Antivirus);
  - Система обеспечения защиты от утечки данных (DLP);
  - Система мониторинга и отслеживания статусов серверов ИСП (Monitoring and Management Service);
- Платежное приложение в виде мобильного приложения для iOS или Android, Веб сайт

платежного приложения, сервис ИСП в виде API.

*3. Определение метода проведения ОТП*

Следующим этапом является, согласование метода проведения ОТП. По умолчанию, ОТП проводится на территории Партнера.

В плане проведения ОТП при выезде согласовываются:

- Дата и время встречи;
- Примерная длительность проведения ОТП, в зависимости от области проведения ОТП;
- Место проведения, адрес площадки Партнера;

В случаях невозможности выезда ТКО на территорию Партнера по операционным причинам, при согласии обеих сторон ОТП проводится посредством удаленного сеанса с использованием заранее согласованного ПО для проведения удаленных встреч.

*4. Подготовка на стороне Партнера*

Партнер со своей стороны начинает подготовку к проведению ОТП. При подготовке Партнер должен:

- Подготовить на ознакомление нормативно-распорядительные документы, определяющие работу ИБ, журналы ознакомления с документами и заявления о предоставлении доступов системным администраторам и разработчикам к сегменту ИСП;
- Подготовить на предоставление логическую топологию сети сегмента ИСП;
- Подготовить данные с межсетевых экранов с области проверки, в виде скриншотов или через веб платформу;
- Подготовить данные о средствах обеспечения ИБ для сегмента ИСП, в виде скриншотов или через веб платформу;
- Подготовить титульные листы последних отчетов по проведению внешних и внутренних сканирований на уязвимость проверяемый сегмент, а также последний отчет о проведенного тестирования на проникновения к сегменту ИСП;
- Подготовить выборки из базы данных СУБД ИСП в виде скриншотов или через веб платформу.

*5. Организация ОТП и анализ соответствия требованиям ТИБ*

На данном этапе проводится ОТП и анализ соответствия ТИБ на основе предоставленных данных со стороны ответственных работников Партнера.

Проверяются все требования, приведенные в ТИБ, перед каждым требованием ставится галочка на один из пунктов

- ✓ «Соответствует» – если требование выполнено полностью;
- ✓ «Частично соответствует» – если требование было выполнено не в полной мере по объективным причинам;
- ✓ «Не соответствует» – если требование не было выполнено;
- ✓ «Неприменимо» – если выполнение требования не соответствует деятельности Партнера;

*6. Заключение и формирование отчетной документации*

После проведения ОТП, на основе предоставленных данных, ТКО в течение 3х рабочих дней подготавливает «Отчет по итогам проведенной ОТП на соответствие требованиям информационной безопасности UZCARD».

При выявлении несоответствий, Партнеру передается перечень с установленными сроками для их устранения.

Партнер проводит устранение выявленных несоответствий и по итогам направляет отчет об устранении несоответствий. В случае, если устранение выявленных несоответствий требует времени более 10 рабочих дней, Партнер направляет гарантийное письмо с указанием сроков устранения несоответствий.

На основе полученных данных, ТКО завершает соответствующий отчет о готовности ИСП на соответствие ТИБ.

**Приложение 2**
к «Регламент проведения организационно-технической проверки на соответствие требованиям информационной безопасности платежной системы UZCARD»

Исходные сведения о Партнере

1. Сведения о Партнере:

| ***Сведения о Партнёре:*** | |
|---|---|
| *1. Форма организации* | |
| *2. Название организации* | |
| *3. Директор / Председатель правления* | |
| *4. Руководитель проекта* | |
| *5. Системный администратор платежного приложения:* | |
| *6. Ответственный по вопросам ИБ платежного приложения:* | |

2. Перечень используемых программных и технических средств:

| ***Наименование*** | ***Описание/Назначение*** |
|---|---|
| ***I. Программные средства*** | |
| *1. Основное платежное средство* | *Приложение "_____", Android, iOS, Web. + версии приложений* |
| *2. Система виртуализации* | *VMWare, ESXi, KVM + версия* |
| *3. ОС сервера* | *Количество серверов, роль (основной, резервный), версия ОС* |
| *4. СУБД* | *Количество серверов, роль (основной, резервный), версия ОС, версия СУБД* |
| *5. Антивирусное ПО* | *Esset, Kaspersky, + (версия)* |
| *6. Система обнаружения вторжений* | *OSSEC, WAZUH, etc + дата последнего обновления* |
| *7. SIEM-система* | *QRadar, OSSIM, etc дата последнего обновления* |
| *8. PAM-система* | *FudoPAM, SingleConnect, One Identity Safeguard, etc дата последнего обновления* |
| *9. Программный межсетевой экран* | |
| *10. ПО балансировщик нагрузки* | *Load Balander, HAPROXY, NGINX, etc.* |
| *11. Веб и\или прокси-сервер* | *HAPROXY, NGINX, etc.* |
| *12.WAP (Web Application Protection) или WAF (Web Application Firewall)* | *NGINX ModSecurity, FortiWAF, Barracuda WAF, Cloudflare WAF* |
| ***II. Технические средства*** | |
| *1. Сетевой маршрутизатор* | |
| *2. Межсетевой экран* | |
| *3. Аппаратный/Программный балансировщик нагрузки* | |
| *4. СКУД (ЦОД)* | |
| *5. СВН (ЦОД)* | |

3. Перечень мест хранения данных платежных карт:

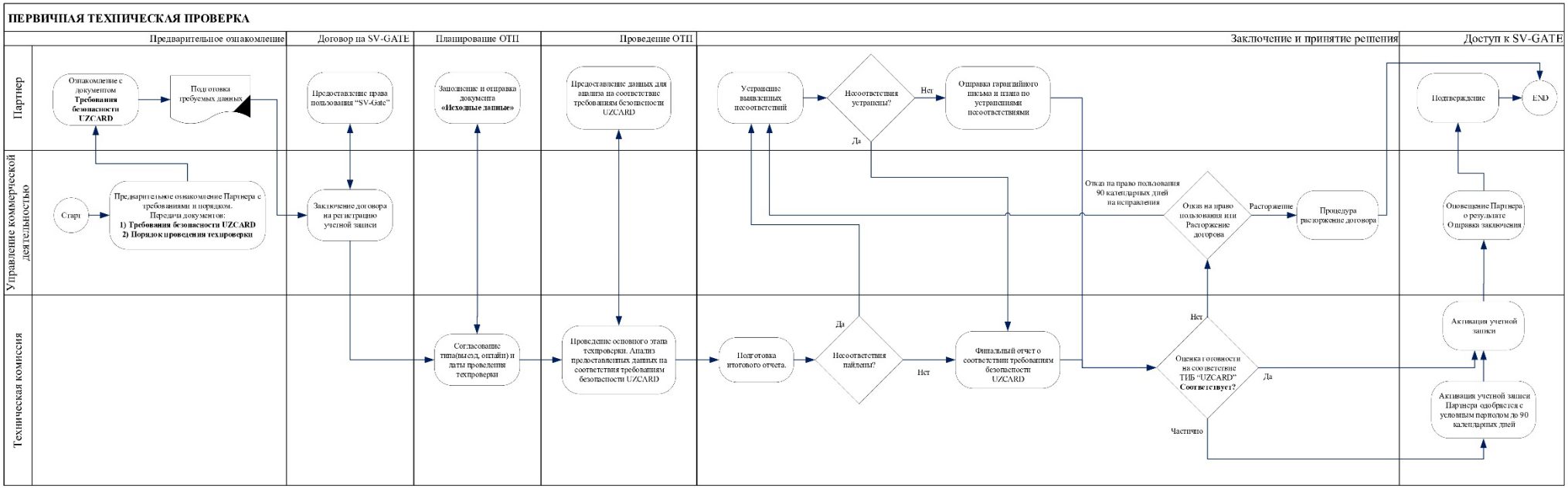
| *№* | *Места хранения* | *Механизм защиты информации* | *Для каких целей* |
|---|---|---|---|
| *1.* | | | |
| *2.* | | | |

4. Перечень нормативно-распорядительных документов Партнера:

| *№* | *Наименование* | *Примечание* |
|---|---|---|
| *1.* | | |
| *2.* | | |

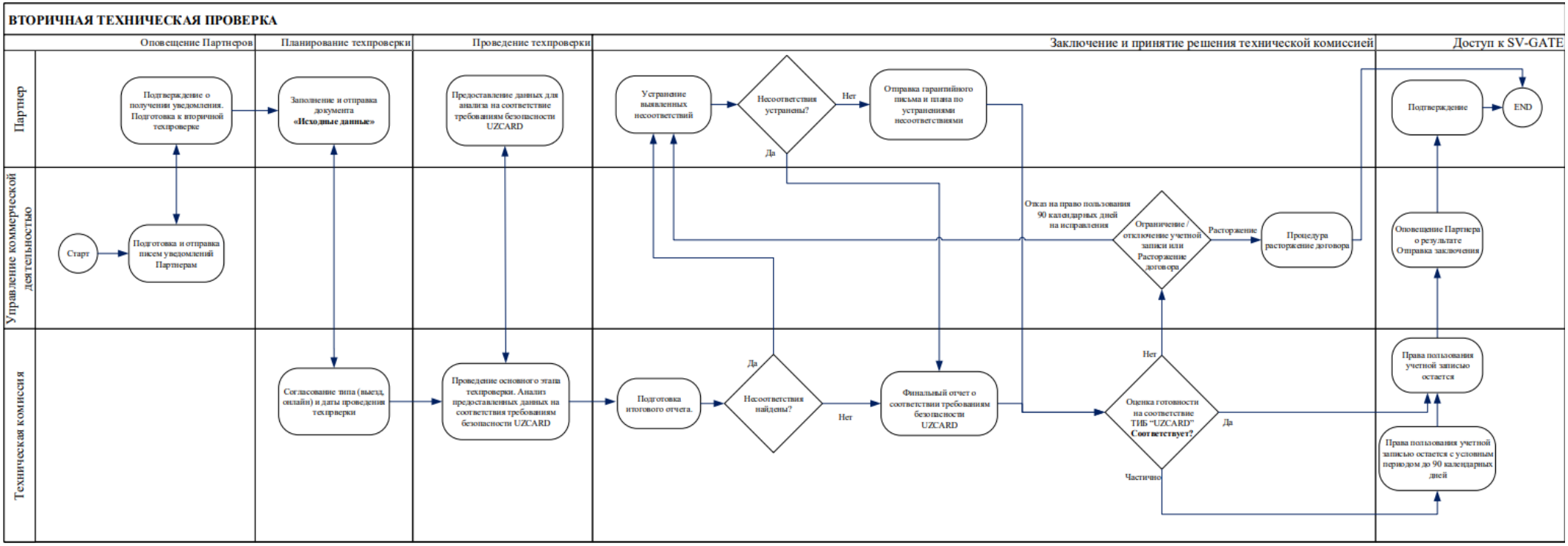
**Приложение 3**
к «Регламент проведения организационно-технической
проверки на соответствие требованиям информационной
безопасности платежной системы UZCARD»

## Схема проведения Первичной ОТП



**Приложение 4**
к «Регламент проведения организационно-технической
проверки на соответствие требованиям информационной
безопасности платежной системы UZCARD»

## Схема проведения Вторичной ОТП



**Приложение 5**
к «Регламент проведения организационно-технической
проверки на соответствие требованиям информационной
безопасности платежной системы UZCARD»

## Схема проведения ОТП путем заполнения Формы