

**Описание функциональных возможностей программного обеспечения  
«Система для управления балансом транспортных карт, регистрации оплаты  
проезда и предоставления информационных сервисов в мобильных приложениях»**

**1. Список сокращений и определений:**

|                      |                                                                                                                                                                                                                                                        |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ТЗ                   | Техническое задание.                                                                                                                                                                                                                                   |
| ПО                   | Используемое в рамках ТЗ программное обеспечение, представляющее собой совокупность программных средств, графической, текстовой, аудио, видео, а также иной цифровой информации.                                                                       |
| АСОП                 | Автоматизированная система оплаты проезда.                                                                                                                                                                                                             |
| Сервис               | Программное обеспечение для серверной системы.                                                                                                                                                                                                         |
| Мобильное приложение | Приложение для операционной системы мобильных устройств.                                                                                                                                                                                               |
| REST API             | Representational State Transfer Application Programming Interface – сетевой программный интерфейс Сервиса для мобильных приложений.                                                                                                                    |
| ОС                   | Операционная система.                                                                                                                                                                                                                                  |
| СУБД                 | Система управления базами данных.                                                                                                                                                                                                                      |
| БД                   | База данных в СУБД.                                                                                                                                                                                                                                    |
| NFC                  | Near Field Communication – технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между мобильным устройством и транспортной картой, находящейся на расстоянии не более 4 сантиметров от устройства. |
| HCE                  | Host Card Emulation – технология для виртуализации карт и совершения бесконтактных платежей мобильным устройством.                                                                                                                                     |

**2. Общие сведения**

2.1. Программное обеспечение обеспечивает доступность для пользователей приложений для мобильных операционных систем Android и iOS. Мобильные приложения предназначены для информирования пользователей и проведения операций с балансом транспортных карт в рамках АСОП.

2.2. Мобильные приложения доступны для установки на мобильные устройства пользователей, удовлетворяющие минимальным требованиям, из электронных магазинов Google Play, RuStore для Android и Apple Store для iOS.

2.3. С помощью мобильных приложений оператор АСОП может предоставлять пользователям различные информационные сервисы и услуги. Мобильные приложения позволяют регистрировать оплату проезда, проводить дистанционные операции с балансом транспортных карт АСОП. Оплачивать данные операции возможно с помощью банковских карт любого банка через интернет-эквайринг или систему быстрых платежей (СБП).

**3. Общие технические требования**

3.1. Сервис и мобильные приложения должны обеспечивать безопасность обрабатываемых данных и сохраняемой информации:

- Безопасность данных Сервиса и мобильных приложений должна быть обеспечена путем применения надежных средств шифрования данных и современных обновленных технологий проектирования и разработки.

- Сервис должен обеспечивать безопасность и конфиденциальность информации, в том числе персональных данных, а также соответствовать требованиям Федерального закона от 27 июля 2006 г. №152-ФЗ «О персональных данных», Постановления Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и от 11.02.2013 г. №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Приказов ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», а также иным требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

- Сервис должен обеспечивать безопасное подключение и создание защищенного канала связи с внешними системами при необходимости подключения к таким системам.

- На системном уровне защита информации должна осуществляться встроенными средствами защиты используемой ОС.

- На уровне СУБД Сервиса защита информации должна осуществляться с использованием механизмов владельцев схем БД, ролей, уникальных идентификаторов и паролей пользователей БД.

- На прикладном уровне защита информации должна обеспечиваться за счет использования средств администрирования в части разграничения прав доступа пользователей к функциям и данным программных компонентов.

- Для целей защиты данных в БД Сервиса от несанкционированного доступа пользователи мобильных приложений не должны иметь доступа непосредственно к СУБД Сервиса.

- Все данные из публичной сети Интернет в сторону Сервиса должны передаваться по протоколу HTTPS с использованием доверенного SSL-сертификата, длина открытого ключа которого не менее 2048 бит для RSA и 256 бит для ECC.

- Мобильные приложения при установке соединения должны проверять принадлежность SSL-сертификата соответствующему домену, а также срок его действия и подлинность.

- Сервис и мобильные приложения не должны локально хранить данные банковских карт пользователей и других платежных систем, которых будет достаточно для совершения платежа при их раскрытии.

3.2. Сервис и мобильные приложения должны обеспечивать надежность работы:

- Надежность работы Сервиса и мобильных приложений должна быть обеспечена путем применения современных и обновленных технологий проектирования и разработки.

- Для защиты от программных и аппаратных сбоев Сервиса должно быть обеспечено резервирование и дублирование критически важных аппаратных средств, с возможностью быстрого переключения без длительной остановки работы Сервиса.

- Программные компоненты и данные Сервиса и ОС сервера периодически должны проходить процедуру резервного копирования в независимое от основной системы безопасное хранилище данных. В случае критического повреждения данных из-за сбоев аппаратного обеспечения или компонентов ОС необходимо провести восстановление данных из резервной копии.

- Сервис должен сохранять работоспособность и обеспечивать восстановление своих функций при возникновении следующих внештатных ситуаций:

- При сбоях в системе электроснабжения аппаратной части, приводящих к перезагрузке ОС. Восстановление работы Сервиса должно происходить после корректного перезапуска ОС и штатного запуска системных программных компонентов.

- При ошибках в работе аппаратных средств (кроме случаев физического или логического сбоя носителей информации сервера). Восстановление функции ПО возлагается на ОС.

- При ошибках, связанных с программным обеспечением (ОС, драйверы устройств, системные компоненты). Восстановление работоспособности возлагается на ОС.

- Возможные отказы и сбои в работе Сервиса не должны приводить к разрушению данных.

- При возникновении сбоев система должна автоматически восстанавливать свою работоспособность после устранения сбоев и корректного перезапуска аппаратного обеспечения (за исключением случаев повреждения рабочих носителей информации с исполняемым программным кодом).

- ПО должно обеспечивать корректную обработку ошибочных ситуаций с возможностью дальнейшего продолжения работы без аварийного закрытия подсистем, за исключением случаев, когда ошибка делает дальнейшую работу невозможной.

#### **4. Функциональные возможности Сервиса и мобильных приложений**

4.1. Сервис должен предоставлять для мобильных приложений REST API в сети интернет по защищенному протоколу HTTPS TLS 1.2 с применением дополнительного слоя сеансовой авторизации и защиты компонентов REST API на базе криптографических алгоритмов на эллиптических кривых. Сессия взаимодействия мобильного приложения и Сервиса должна быть ограничена по времени, по истечении которого требуется повторная авторизация для открытия новой сессии. Множественные попытки неуспешной авторизации должны приводить к временной блокировке пользователя или устройства.

4.2. Сервис состоит из функциональных модулей, доступных мобильным приложениям по REST API:

4.2.1. Системный журнал.

4.2.2. Пользователь и система его авторизации.

4.2.3. Профиль пользователя.

4.2.4. Контактная информация службы поддержки пользователей АСОП.

4.2.5. Географические карты пунктов обслуживания в различных городах и населенных пунктах.

4.2.6. Новости.

4.2.7. Вопросы и ответы.

4.2.8. Обратная связь.

4.2.9. Дополнительные сервисы.

4.2.10. Баннеры для главного экрана мобильных приложений.

4.2.11. Модуль операций с транспортными картами:

4.2.11.1. Типы поддерживаемых транспортных карт АСОП: MIFARE Classic, CIPURSE., виртуальная транспортная карта (HCE).

4.2.11.2. Режимы работы с транспортной картой: по номеру транспортной карты, по физической или виртуальной транспортной карте, считанной соответственно по NFC или HCE мобильным устройством с поддержкой данного типа карт.

4.2.11.3. Типы операций с балансом транспортной карты: проверка баланса, пополнение баланса по текущему тарифу, смена тарифа на транспортной карте (возможна только в режиме работы с картой по NFC или HCE), оплата оформленной операции с балансом транспортной карты через интернет-эквайринг, оплата оформленной операции с балансом транспортной карты через систему быстрых платежей (СБП), запись оформленной и оплаченной операции на транспортную карту,

4.2.11.4. История операций с транспортными картами, оформленных в мобильных приложениях, привязанных к профилю пользователя.

4.2.11.5. Избранные транспортные карты пользователя.

4.2.11.6. История поездок по транспортным картам.

4.2.12. Административный интерфейс для отслеживания внутреннего состояния, внешних запросов, оформленных в мобильных приложениях операций с транспортными картами, для управления пользователями и мобильными устройствами, а также для дистанционного информационного наполнения различных разделов мобильных приложений.

4.3. Минимально поддерживаемые версии мобильных операционных систем следующие: Android – версия 5.0 и выше, iOS – версия 13 и выше.

4.4. Мобильные приложения должны быть нативными и разрабатываться с применением стандартных инструментальных средств, поставляемых производителями мобильных операционных систем.

4.5. Интерфейс, дизайн и эргономика мобильных приложений должны быть реализованы в соответствии с ГОСТ Р ИСО 9241-210-2012 «Эргономика взаимодействия человек-система. Часть 210. Человеко-ориентированное проектирование интерактивных систем» и официальными рекомендациями производителей мобильных операционных систем по разработке приложений: iOS Human Interface Guidelines для iOS и Android Design Principles для Android. Интерфейс мобильных приложений должен быть адаптивным к различным размерам экранов устройств.

4.6. Все мобильные приложения должны соответствовать формальной процедуре проверки (модерации) производителей мобильных ОС перед процедурой публикации в магазинах приложений.

4.7. Мобильные приложения должны взаимодействовать с Сервисом по REST API в сети интернет по защищенному протоколу HTTPS TLS 1.2 с применением дополнительного слоя сеансовой авторизации и защиты компонентов REST API на базе криптографических алгоритмов на эллиптических кривых.

4.7.1. Мобильные приложения должны функционировать как при наличии подключения к сети интернет, так и при его отсутствии.