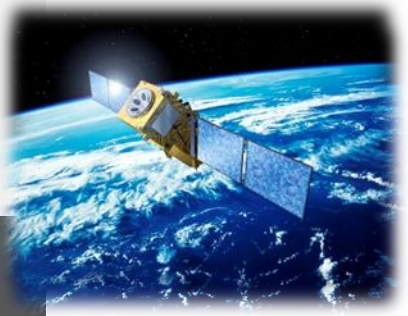








Криптография в цифровых тахографах

Москва, 2026 г.

ПОНЯТИЯ И ПРАВОВЫЕ ОСНОВАНИЯ

- **Федеральный закон от 10.12.1995 № 196-ФЗ «О безопасности дорожного движения»**

Тахограф - техническое средство контроля, обеспечивающее непрерывную, **некорректируемую регистрацию информации** о рабочем времени водителя транспортного средства, времени управления транспортным средством, времени отдыха водителя транспортного средства, скорости, маршруте движения транспортного средства, а также запись данных из блока криптографической защиты информации, входящего в состав тахографа, на карты водителя транспортного средства, контролера, предприятия и мастерской по оснащению транспортных средств тахографами и обслуживанию тахографов (далее - мастерская тахографов). (**Статья 2. Основные термины)**

- **Приказ Минтранса России от 28.10.2020 № 440 "Об утверждении требований к тахографам, устанавливаемым на транспортные средства, категорий и видов транспортных средств, оснащаемых тахографами, правил использования, обслуживания и контроля работы тахографов, установленных на транспортные средства».**

Тахограф должен обеспечивать регистрацию в **некорректируемом** виде данных о скорости и маршруте движения транспортного средства, времени управления транспортным средством и времени отдыха водителей транспортных средств, режиме труда и отдыха водителей транспортных средств, управление которыми входит в их трудовые обязанности, созданием **квалифицированной электронной подписи,** присоединяемой к защищаемым данным, и разграничение доступа к защищаемой информации с использованием шифровальных (криптографических) средств. **(пункт 83 Требований к тахографам, устанавливаемым на транспортные средства)**

НЕКОРРЕКТИРУЕМОСТЬ

- **Некорректируемая регистрация информации:**
- Способ обработки информации средством регистрации, по результатам которой обеспечиваются:
- регистрация информации в соответствии с установленным перечнем;
- идентичность зарегистрированной информации с информацией, предназначенной для регистрации (формирования и/или записи), хранения и/или передачи;
- непрерывность регистрации (защита от нарушения последовательности регистрации блоков информации);
- возможность гарантированного выявления фактов корректировки или фальсификации информации по результатам проверки, в том числе и фактов нарушения последовательности зарегистрированных событий (непрерывности регистрации);
- возможность гарантированной аутентификации средства регистрации.
- **Результат:**
- Обеспечение конфиденциальности информации, аутентификации (данных, источника данных, стороны), контроля целостности данных, невозможности отрицания создания или получения информации.

КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ (ГОСТ Р 34.14-2025). ТЕРМИНЫ

Криптографическая защита информации: Защита информации с помощью ее криптографического преобразования.

Средства криптографической защиты информации; СКЗИ: Средства, системы и комплексы, реализующие криптографическую систему или отдельные криптографические механизмы.

Примечание — К средствам криптографической защиты информации относятся средства шифрования, средства имитозащиты, средства электронной подписи, средства кодирования, средства изготовления ключевых документов, ключевые документы.

криптографический алгоритм: Алгоритм, описывающий процесс криптографического преобразования информации. Входом криптографического алгоритма являются изменяемые данные, которые могут включать открытый или шифрованный текст, криптографический ключ или ключевой материал.

Цифровая подпись: Результат криптографического преобразования набора данных (сообщения), зависящего от ключа подписи и параметров схемы цифровой подписи, обеспечивающий возможность аутентификации данных и невозможность отрицания факта создания.

Квалифицированный сертификат (ключа проверки электронной подписи): Сертификат ключа проверки электронной подписи, выданный аккредитованным удостоверяющим центром либо федеральным органом исполнительной власти, уполномоченным в сфере использования электронной подписи, и являющийся в связи с этим официальным документом.

Криптографическая система аутентификации стороны: Криптографическая система, предназначенная для обеспечения аутентификации стороны, включающая в себя криптографический протокол аутентификации стороны и ключевую систему.

Среда функционирования средства криптографической защиты информации; Совокупность одного или нескольких аппаратных средств и программного обеспечения, совместно с которыми штатно функционирует средство криптографической защиты информации и которые способны повлиять на выполнение предъявляемых к нему требований.

ПЕРЕЧЕНЬ ГОСТ, НА ОСКОВАНИИ КОТОРЫХ СФОРМУЛИРОВАНЫ ТЕРМИНЫ

ГОСТ Р 7.0.8-2025 Система стандартов по информации, библиотечному и издательскому делу. Делопроизводство и архивное дело. Термины и определения

ГОСТ Р 34.10-2012 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования

ГОСТ Р 34.12-2015 Информационная технология. Криптографическая защита информации. Блочные шифры

ГОСТ Р 34.13-2015 Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров

ГОСТ Р 50922-2006 Защита информации. Основные термины и определения

ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели

ГОСТ Р 56136-2014 Управление жизненным циклом продукции военного назначения. Термины и определения

ГОСТ Р 56498- 2015/IEC/PAS 62443-3:2008 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3 Защищенность (кибербезопасность) промышленного процесса измерения и управления

ГОСТ Р 57149/ISO/IEC Guide 51:2014 Аспекты безопасности. Руководящие указания по включению их в стандарты

Приказ Минтранса России № 440. Требования к тахографам.

4. Тахограф должен обеспечивать целостность и достоверность информации, регистрируемой в памяти блока СКЗИ тахографа в некорректируемом виде, на основе применения квалифицированной электронной подписи, а также возможность гарантированного выявления ее корректировки или фальсификации по результатам проверки информации, зарегистрированной в памяти блока СКЗИ тахографа.

83. Тахограф должен обеспечивать регистрацию в некорректируемом виде данных о скорости и маршруте движения транспортного средства, времени управления транспортным средством и времени отдыха водителей транспортных средств, режиме труда и отдыха водителей транспортных средств, управление которыми входит в их трудовые обязанности, созданием квалифицированной электронной подписи, присоединяемой к защищаемым данным, и разграничение доступа к защищаемой информации с использованием шифровальных (криптографических) средств.

84. Реализация криптографических алгоритмов, необходимых для шифрования и расшифровывания информации, вычисления квалифицированной электронной подписи, проведения процедур аутентификации и обеспечения защиты информации, регистрируемой, обрабатываемой и хранимой в тахографе, и подлежащей защите в соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ "О персональных данных" и пунктом 83 Требований, должна осуществляться блоком СКЗИ тахографа и картами.

85. Разработка блока СКЗИ тахографа и карт должна осуществляться в соответствии с Положением ПКЗ-2005.

90. Тематические исследования карт и блоков СКЗИ тахографа, в том числе в составе тахографа, на соответствие требованиям по безопасности информации должны осуществляться в соответствии с Положением ПКЗ-2005.

БЛОК СКЗИ И КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Блок СКЗИ тахографа:

1. Программно-аппаратное шифровальное (криптографическое) средство, реализующее алгоритмы криптографического преобразования информации и обеспечивающее:

аутентификацию водителя, Государственной инспекции безопасности дорожного движения Министерства внутренних дел Российской Федерации или Федеральной службы по надзору в сфере транспорта, в том числе их территориальных органов (далее - контрольные органы), сервисного центра (далее - мастерская, если не указано иное), юридических лиц, индивидуальных предпринимателей, осуществляющих эксплуатацию транспортных средств, а также физических лиц, осуществляющих эксплуатацию грузовых автомобилей, разрешенная максимальная масса которых превышает 3,5 тонн, и автобусов (далее - владельцы транспортных средств), а также соответствующих карт;

регистрацию информации в некорректируемом виде в защищенной памяти (далее - защищенный архив блока СКЗИ тахографа);

хранение информации ограниченного доступа, используемой для создания электронной подписи и проверки электронной подписи (далее - ключевая информация).

2. Блок СКЗИ тахографа в составе бортового устройства с функцией передачи данных обеспечивает:

автоматическое формирование, подписание квалифицированной электронной подписью водителя и передачу в зашифрованном и некорректируемом виде информации, регистрируемой тахографом, в автоматизированную информационную систему "Тахографический контроль»;

формирование и передачу в информационную систему заявления, содержащего сведения об активизации блока СКЗИ тахографа, корректировке установочных данных и (или) идентификационных данных транспортного средства, подписанного квалифицированной электронной подписью владельца карты предприятия или владельца карты мастерской.

КАРТЫ ТАХОГРАФА И КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

КАРТЫ ТАХОГРАФОВ:

1) карта водителя - обеспечивает идентификацию и аутентификацию водителя с использованием шифровальных (криптографических) средств, а также хранение данных о деятельности водителя;

2) карта контролера - обеспечивает идентификацию и аутентификацию контрольных органов с использованием шифровальных (криптографических) средств, а также хранение данных, предусмотренных Требованиями;

3) карта мастерской - обеспечивает идентификацию и аутентификацию мастерской с использованием шифровальных (криптографических) средств, а также хранение данных, предусмотренных Требованиями;

4) карта предприятия - обеспечивает идентификацию и аутентификацию владельцев транспортных средств с использованием шифровальных (криптографических) средств, установку блокировки (ограничения) доступа к данным тахографа и данным карт водителей, а также хранение данных, предусмотренных Требованиями.

91. Создание карт, создание и выдача квалифицированных сертификатов карт, выполнение иных, необходимых для выполнения указанных работ функций, предусмотренных Федеральным законом от 6 апреля 2011 г. N 63-ФЗ "Об электронной подписи", должны выполняться организациями, соответствующими требованиям законодательства Российской Федерации к организациям, осуществляющим данный вид деятельности.

94. Карты контролера, мастерской и предприятия должны содержать квалифицированный сертификат, определяющий полномочия держателя карты при доступе к данным тахографа, к данным защищенного архива блока СКЗИ тахографа и данным карты водителя.

КРИПТОГРАФИЯ ПРИ АКТИВИЗАЦИИ ОНЛАЙН-ТАХОГРАФА

96(1) Тахограф, имеющий в своем составе бортовое устройство с функцией передачи данных, при активизации блока СКЗИ тахографа, установке и извлечении блока СКЗИ тахографа, корректировке установочных данных и (или) идентификационных данных транспортного средства должен обеспечивать:

1) формирование и передачу в информационную систему заявления, содержащего сведения об активизации блока СКЗИ тахографа, корректировке установочных данных и (или) идентификационных данных транспортного средства, подписанного квалифицированной электронной подписью владельца карты предприятия или владельца карты мастерской (далее - заявление о настройке тахографа);

2) получение подтверждения информационной системы о возможности активизации блока СКЗИ тахографа, корректировки установочных данных и (или) идентификационных данных транспортного средства на основании заявления о настройке тахографа, автоматически подписанного квалифицированной электронной подписью информационной системы (далее - подтверждение по заявлению);

3) корректировку установочных данных и (или) идентификационных данных транспортного средства при получении подтверждения по заявлению;

КРИПТОГРАФИЯ ПРИ АКТИВИЗАЦИИ ОНЛАЙН-ТАХОГРАФА (продолжение)

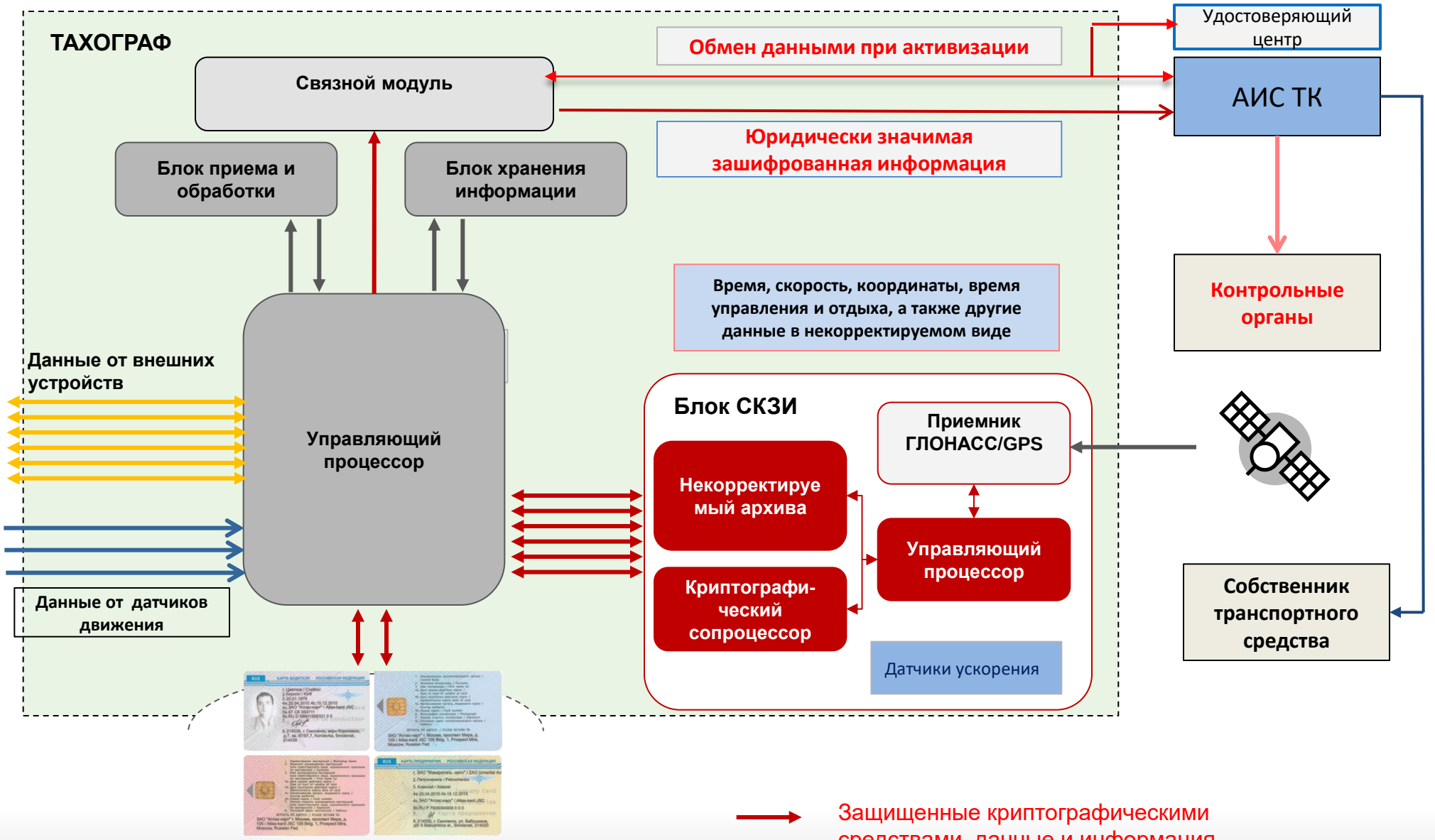
4) формирование и передачу в удостоверяющий центр или доверенному лицу удостоверяющего центра запроса на создание квалифицированного сертификата, подписанного квалифицированной электронной подписью владельца карты предприятия или владельца блока СКЗИ тахографа при получении от информационной системы подтверждения по заявлению

5) активизацию блока СКЗИ тахографа при получении квалифицированного сертификата;

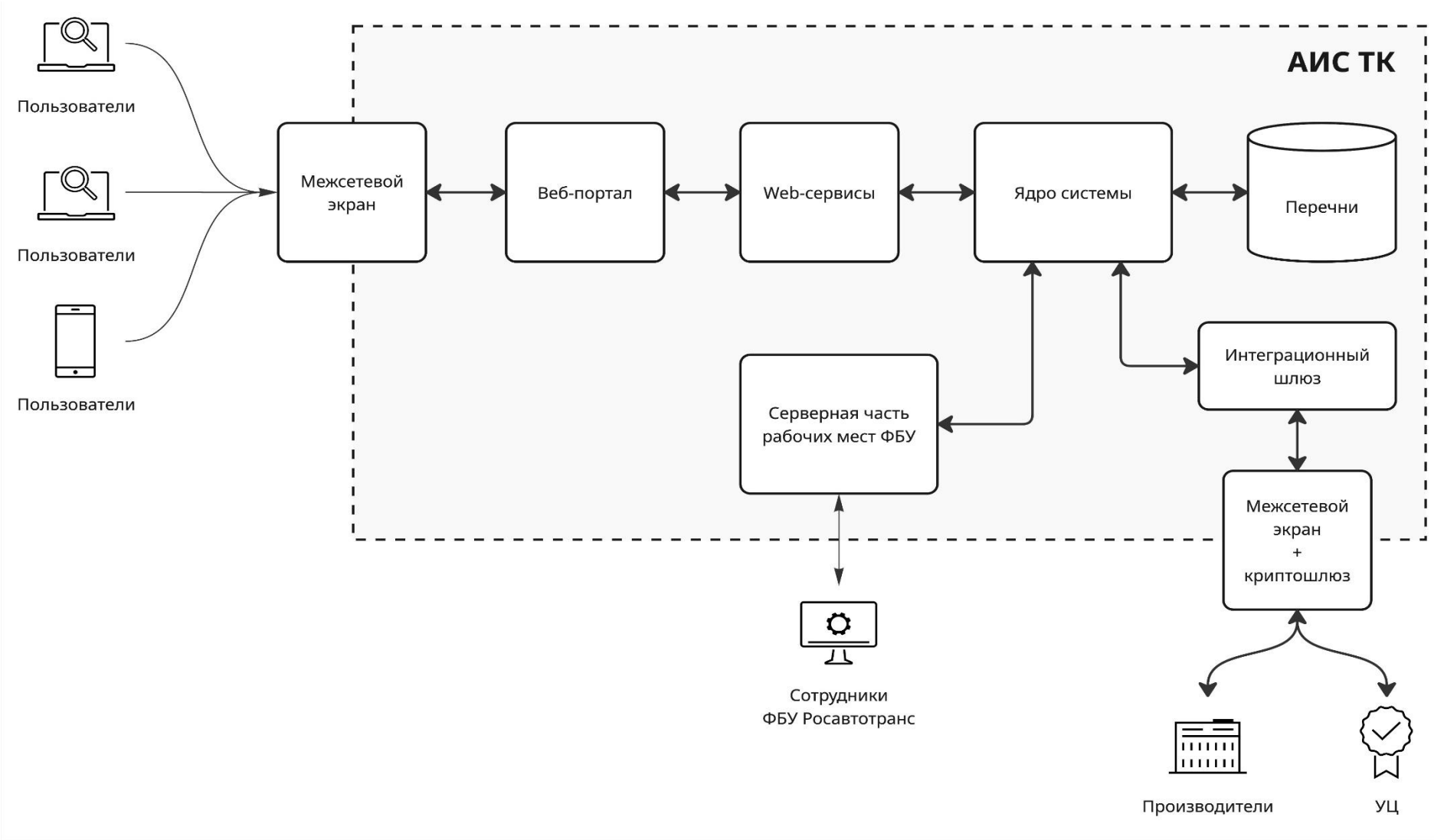
6) формирование и передачу в информационную систему уведомления об активизации блока СКЗИ тахографа, установке и извлечении блока СКЗИ тахографа, корректировке установочных данных и (или) идентификационных данных транспортного средства после завершения активизации блока СКЗИ тахографа, уведомления об установке и извлечении блока СКЗИ тахографа, корректировки установочных данных;

7) получение подтверждения информационной системы о внесении изменений в сведения о тахографе, содержащиеся в соответствующих перечнях о тахографах и блоках СКЗИ тахографа (далее - подтверждение по уведомлению), запись данных о получении подтверждения по уведомлению в защищенный архив блока СКЗИ тахографа, и вывод на дисплей тахографа соответствующего оповещения о завершении активизации блока СКЗИ тахографа, о принятии уведомления об установке и извлечении блока СКЗИ тахографа, корректировке установочных данных и (или) идентификационных данных транспортного средства, а также о допуске тахографа к применению на данном транспортном средстве.

ОБЩАЯ СХЕМА ОНЛАЙН ТАХОГРАФА

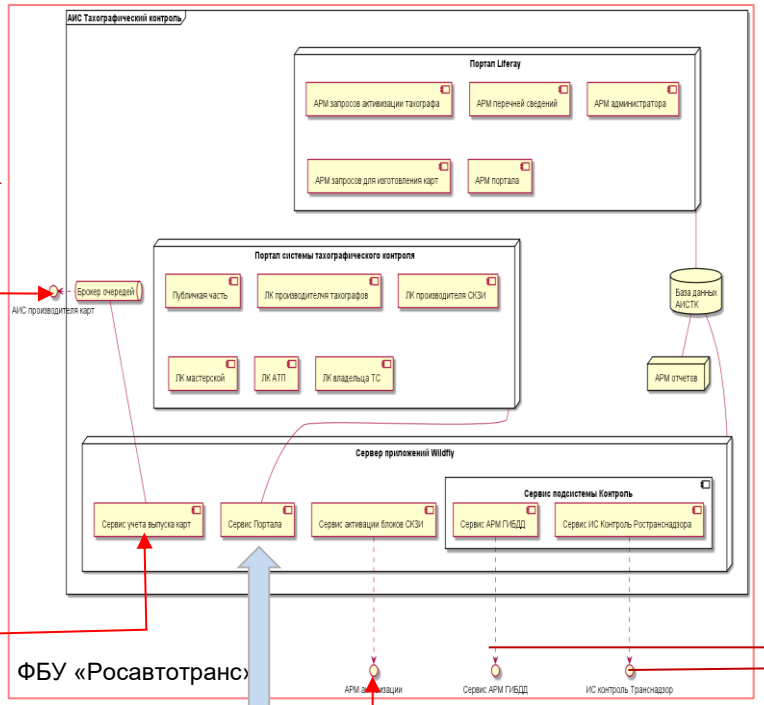


ПРИМЕРНАЯ СХЕМА ИНФОРМАЦИОННОГО ОБМЕНА



ОБЩАЯ СХЕМА ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ





МВД России

ГИБДД

Ространснадзор

Организации-изготовители карт

Водитель (иной пользователь карты тахографа)

Организации-изготовители блоков СКЗИ тахографа

Удостоверяющий центр (УЦ)

Мастерская (доверенное лицо УЦ

Собственник (доверенное лицо) Транспортного средства

СПАСИБО ЗА ВНИМАНИЕ!

Россия, Москва, 129626, Кулаков переулок дом 9, стр.1