Некоммерческое партнерство
«Содействие развитию и использованию навигационных технологий»

УТВЕРЖДАЮ

Президент

_____/ А.О. Гурко

«____» _____2020 г.

М.П.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

на СЧ НИР «Проектирование Платформы «Автодата», разработка технического проекта в части разработки материалов в концепцию платформы «Кибербезопасность»

СОГЛАСОВАНО

Главный конструктор

_____/ А.А. Разговоров

«____» _____2020 г.

Москва 2020

Оглавление

Оглавление

1 Общие сведения

1.1 Полное наименование системы, проекта, этапа реализации проекта

Полное наименование системы: Информационная система «Платформа «Автодата».

Полное наименование проекта: создание, внедрение и ввод в постоянную эксплуатацию российской сервисной навигационно-телематической платформы, обеспечивающей формирование национального массива статистических и аналитических данных (больших данных) о колесных транспортных средствах, дорожной инфраструктуре, поведенческих моделях пассажиров и водителей, и иной информации в транспортной сфере, в том числе связанной с логистикой людей и вещей (Платформа «Автодата»).

Наименование этапа - СЧ НИР «Проектирование Платформы «Автодата», разработка технического проекта в части разработки материалов в концепцию платформы «Кибербезопасность».

1.2 Сокращенное наименование системы

Сокращенные наименования системы: Платформа «Кибербезопасность», Система.

1.3 Наименование разработчика

Заказчик: НП «Содействие развитию и использованию навигационных технологий».

Разработчик: выбирается по результатам конкурсных процедур.

1.4 Перечень документов, на основании которых создается система, кем и когда утверждены эти документы

Протоколы заседаний Межведомственной рабочей группы по разработке и реализации Национальной технологической инициативы при Правительственной комиссии по модернизации экономики и инновационному развитию России от 7 августа 2019 г. № 2, и от 06.11.2020 №4.

1.5 Плановые сроки начала и окончания работы по созданию системы

Дата начала работ: с даты подписания договора.

Плановый срок окончания работ: 20.03.2021.

1.6 Порядок оформления и предъявления результатов работ

Состав, содержание, термины и определения, являющихся результатами работ должно соответствовать стандартам на автоматизированные системы: ГОСТ 34.602-89, ГОСТ 34.601-90, ГОСТ 34.003-90.

Результаты работ должны быть переданы в порядке, представленном в разделе 5 «Требования к документации» настоящего Технического задания.

Материалы в концепцию платформы «Кибербезопасность» должны быть переданы в одном экземпляре на бумажном носителе и в одном экземпляре на электронном носителе.

Текстовые документы, передаваемые на электронном носителе, должны быть представлены в форматах MS Office.

Если в состав материалов в концепцию платформы «Кибербезопасность» войдут материалы, требующие больших форматов (схемы, чертежи, фотоматериалы и пр.), то выполнение приложений к таким документам может быть предоставлено только на электронном носителе в форматах Adobe PDF, TIFF, JPEG и др. При этом основная часть документа должна быть выпущена в соответствии с требованиями, определенными выше.

Все материалы должны быть переданы с сопроводительными документами Разработчика.

1.6.1 **Сведения об использованных нормативно-технических документах**

При разработке материалов в концепцию платформы «Кибербезопасность» необходимо использовать следующие нормативно-технические документы:

- ГОСТ 19.001-77 Единая система программной документации. Общие положения;
- ГОСТ 19.103-77 Единая система программной документации. Обозначения программ и программных документов;
- ГОСТ 19.104-77 Единая система программной документации. Основные надписи;
- ГОСТ 19.105-77 Единая система программной документации. Общие требования к программным документам;
- ГОСТ 19.301-77 Единая система программной документации. Программа и методика испытаний;
- ГОСТ 19.404-77 Единая система программной документации. Пояснительная записка;
- ГОСТ Р ИСО МЭК 12207-2010 Информационные технологии. Системная и программная инженерия. Процессы жизненного цикла программных средств;
- ГОСТ Р ИСО/МЭК ТО 15271-2002. Информационная технология. Руководство по применению ГОСТ Р ИСО/МЭК 12207 (Процессы жизненного цикла программных средств);
- ГОСТ 28806-90 Качество программных средств. Термины и определения;
- ГОСТ 28195-89 Оценка качества программных средств. Общие положения;
- ГОСТ Р ИСО/МЭК 9126:1993 Информационная технология. Оценка программной продукции. Характеристики качества и руководство по их применению;
- ГОСТ Р ИСО/МЭК 12119-2000 Информационная технология. Пакеты программ. Требование к качеству и тестирование;
- ГОСТ Р ИСО/МЭК ТО 9294-93 Информационная технология. Руководство по управлению документированием программного обеспечения;
- ГОСТ Р ИСО 9127:1994 Системы обработки информации. Документация пользователя и информация на упаковке для потребительских программных пакетов;
- ГОСТ Р ИСО/МЭК 15910-2002 Информационная технология. Процесс создания документации пользователя программного средства;

- ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности;
- ГОСТ Р ИСО/МЭК 14764-2002 Информационная технология. Сопровождение программных средств;
- ГОСТ Р ИСО/МЭК 15026-2002 Информационная технология. Уровни целостности систем и программных средств;
- ГОСТ Р ИСО/МЭК ТО 12182-2002 Информационная технология. Классификация программных средств;
- ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель;
- ГОСТ 19781-90 Обеспечение систем обработки информации программное. Термины и определения;
- ГОСТ 24.301-80 Система технической документации на АСУ. Общие требования к выполнению текстовых документов;
- ГОСТ 34.003 (актуальная реализация) Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения;
- ГОСТ 34.201 (актуальная реализация) Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;
- ГОСТ 34.601 (актуальная реализация) Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадия создания;
- ГОСТ 34.603 (актуальная реализация) Информационная технология. Виды испытаний автоматизированных систем;
- ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования;
- ГОСТ 27.301-95 Надежность в технике. Расчет надежности. Основные положения;
- ГОСТ 27.402-95 Надежность в технике (ССНТ). Планы испытаний для контроля средней наработки до отказа (на отказ);
- ГОСТ Р 27.403-2009 Надежность в технике. Методы контроля показателей надежности и планы контрольных испытаний на надежность.

2 Назначение и цели разработки материалов в концепцию платформы «Кибербезопасность»

В целях разработки требований к используемым технологиям, способам и средствам защиты информации, формируемой на борту транспортных средств и передаваемой в Платформу «Автодата» через телематические платформы участников рынка и подсистемы ИТС (V2X), разрабатывается концепция информационной безопасности платформы «Кибербезопасность». В рамках разработки концепции должны быть описаны комплексные меры защиты и обеспечения безопасности данных на этапах их формирования в электронных системах и компонентах автомобиля, передачи посредством автомобильного бортового телематического оборудования и бортового оборудования V2X, хранения и обработки данных в телематических платформах автопроизводителей и других участников рынка, а также в подсистемах ИТС (V2X), включая анализ информационных потоков, уязвимых звеньев и возможных угроз безопасности информации, оценку ущерба от реализации угроз, анализ имеющихся в распоряжении мер и средств защиты информации, определения основных рекомендаций направлений и способов защиты информации, а также решение вопросов обеспечения защиты информационных ресурсов.

Кроме того, целью разработки концепции платформы «Кибербезопасность» является создание основы для разработки нормативной правовой и нормативно-технической базы в части требований к транспортным средствам, выпускаемым в обращение на территории РФ, по наличию функциональности по сбору и некорректируемой передаче в обязательном порядке данных от электронных систем и компонентов транспортных средств в Платформу «Автодата» через телематические платформы, эксплуатируемые на территории РФ автопроизводителями, сервис-провайдерами и другими участниками рынка, а также через подсистемы ИТС (V2X).

В ходе выполнения работ по разработке материалов в концепцию платформы «Кибербезопасность» должны быть проведены технические исследования, необходимые для разработки нормативных документов и документов технического регулирования во взаимодействии с учредителями и участниками Межотраслевого международного проектного консорциума «АВТОДАТА.РУС».

По результатам разработки концепции платформы «Кибербезопасность» на следующих этапах проекта планируется разработка и отработка ключевых технических решений, предназначенных для обеспечения защиты от несанкционированного доступа, искажения, подмены или компрометации данных, формируемых и передаваемых между электронными системами и компонентами транспортных средств, передаваемых по сетям подвижной радиотелефонной связи 3G/4G/5G через телематические платформы, по каналам беспроводной связи V2X (ITS-G5 и C-V2x) через подсистемы ИТС (V2X) в Платформу «Автодата». Разрабатываемые технические решения лягут в основу платформы «Кибербезопасность», создаваемую с учетом современных и перспективных требований к защите информации и обеспечению информационной безопасности.

3 Характеристика объектов автоматизации

При разработке материалов в концепцию платформы «Кибербезопасность» должны быть разработаны требования к:

- защите данных как на основе перспективных стандартов и архитектур электронных систем и компонентов, включая платформу AUTOSAR Adaptive, так и на основе существующих в настоящее время вариантов реализации электронных систем и компонентов транспортных средств;
- программному модулю (специализированному приложению «Автодата»), функционирующему на борту транспортного средства и обеспечивающему сбор и защиту данных, подлежащих обязательной передаче в Платформу «Автодата» через телематические платформы и подсистемы ИТС (V2X);
- программным модулям телематических платформ, подсистем ИТС (V2X), к инфраструктуре аутентификаторов, обеспечивающим защищенную передачу информации, получаемую от транспортных средств, в Платформу «Автодата»;
- подсистеме Платформы «Автодата», обеспечивающей загрузку на борт транспортного средства специализированного приложения «Автодата», его обновления и управления настройками в целях поддержки процессов сбора и защищенной передачи данных из транспортных средств через телематические платформы и подсистемы ИТС (V2X) в Платформу «Автодата».

4 Требования к выполняемым работам

4.1 Анализ угроз и решений по кибербезопасности подключенного автомобиля

Материалы в концепцию платформы «Кибербезопасность» должны включать:

- цели и задачи защиты информации на всех уровнях, а именно, на уровне электронных систем и компонентов транспортных средств, на уровне телематических платформ, на уровне дорожного оборудования V2X, подсистем ИТС (V2X), и на уровне Платформы «Автодата»;
- описание объектов защиты, идентифицируемых в ходе разработки модели угроз концепции информационной безопасности платформы «Кибербезопасноть»;
- разработку модели угроз и нарушителя информационной безопасности;
- методы обеспечения информационной безопасности;
- организационные и технические мероприятия по защите информации;
- описание параметров и критериев контроля эффективности защиты информации.

Разрабатываемые материалы в концепцию платформы «Кибербезопасность» должны содержать анализ сценариев несанкционированного вмешательства:

- в работу электронных систем и компонентов транспортного средства через внутренние и внешние сетевые соединения, в работу бортового электронного оборудования, имитирующие атаки через радиоканалы (например, шлюз бортового медиа-центра), через подключение к технологическому разъёму OBD-II, например, перехват управления – атака на бортовые контроллеры, подмена телематических данных – атака на бортовое телематическое оборудование и других сценариев, определяемых в разрабатываемой модели угроз информационной безопасности;
- в работу телематических платформ, осуществляющих сбор данных из транспортных средств через сети подвижной радиотелефонной связи (3G/4G/5G);
- в работу дорожного оборудования V2X и подсистем ИТС (V2X).

На основе произведенного анализа разрабатываемые материалы должны содержать:

- описание (модель) угроз информационной безопасности, которые могут привести к нарушению конфиденциальности, целостности, доступности, подлинности и/или неотказуемости информации на всех уровнях ее сбора и обработки, а именно:
    1) на уровне электронных систем и компонентов транспортных средств;
    2) на уровне автомобильного бортового телематического и бортового оборудования V2X;
    3) на уровне телематических платформ;
    4) на уровне дорожного оборудования V2X и подсистем ИТС (V2X);
    5) на уровне Платформы «Автодата».

- необходимые материалы для согласования разработанной модели угроз информационной безопасности с российским регулятором в области информационной безопасности;
- предложения по доработке, в случае необходимости, существующей международной нормативной базы и локальных нормативных актов в части требований к защите информации при ее формировании электронными бортовыми системами транспортного средства, передаче информации посредством различных технологий связи, сборе, хранении и обработке информации в информационных системах автопроизводителей, сервис-провайдеров и других участников рынка;
- анализ существующих технических решений по защите информации, реализуемых для обеспечения конфиденциальности, целостности, доступности, подлинности и неотказуемости данных при их формировании бортовыми электронными системами и компонентами транспортного средства, передаче данных посредством различных технологий связи, сборе, хранении и обработке информации информационными системами автопроизводителей, сервис-провайдеров и других участников рынка.

4.2 Требования к обеспечению кибербезопасности на борту автомобиля

В рамках разработки материалов в концепцию платформы «Кибербезопасность» должны быть разработаны требования и материалы в частное техническое задание на платформу «Кибербезопасность» в части защиты информации от бортовых электронных систем и компонентов транспортных средств, включая бортовое телематическое оборудование.

Требования к платформе «Кибербезопасность» в части защиты данных на борту транспортного средства должны учитывать перспективные международные стандарты и архитектуры электронных систем и компонентов транспортных средств, включая платформу AUTOSAR Adaptive, а также стандарты, используемые в автомобилях с традиционной архитектурой электронных компонентов и систем, и включать:

- требования и описание сценариев защиты внутреннего обмена данными и командами различных бортовых электронных систем и компонентов автомобиля, передачи данных во внешние системы по сетям подвижной радиотелефонной связи 2G/3G/4G и по каналам беспроводной связи V2X (ITS-G5 и C-V2x);
- анализ вариантов реализации защиты информации на борту транспортного средства, предусматриваемых перспективными международными стандартами и архитектурами, включая платформу AUTOSAR Adaptive и выбор наиболее подходящего с учетом разнообразия транспортных средств, выпускаемых в обращение в России;
- обоснование выбранного варианта или вариантов реализации защиты информации на борту транспортного средства;
- требования к специализированному приложению «Автодата», являющегося составной частью платформы «Кибербезопасность», в части:

1. загрузки приложения «Автодата» по каналам беспроводной связи или иными способами на борт транспортного средства, верификации подлинности и целостности его кода, установки и выполнения приложения в защищённом режиме;
2. управления настройками и конфигурацией приложения «Автодата» в части сбора, обеспечения защиты данных от электронных систем и компонентов транспортного средства, например, таких данных, как координаты, направление движения и скорость, данных удалённой диагностики (наличие кодов неисправностей) и других данных, подлежащих передаче в Платформу «Автодата».
3. портируемости приложения «Автодата» для различных вариантов сред исполнения приложений, реализованных в различных транспортных средствах;
4. возможности адаптации/доработки приложения «Автодата» под нужды автопроизводителя для наращивания его функционала, например, реализации прикладных сервисов провиженинга бортового оборудования (аутентификации, сохранение аутентификаторов и системных параметров), сбора, защиты и передачи данных, требуемых для автопроизводителя.

В рамках разработки материалов в частное техническое задание на платформу «Кибербезопасность» в части защиты электронных систем и компонентов транспортного средства, функционирующих с учетом выбранного варианта как перспективной, так и существующей архитектуры электронных систем и компонентов транспортного средства, должны быть описаны функциональные и технические требования к:

1. программному модулю, реализующему функции по защите данных, передаваемых между электронными системами и компонентами транспортного средства по шинам передачи данных;
2. бортовому телематическому оборудованию (автомобильному коммуникационному шлюзу), обеспечивающему обмен данными с внешними по отношению к транспортному средству информационными системами через сети подвижной радиотелефонной связи 2G/3G/4G/5G;
3. бортовому оборудованию V2X, обеспечивающему обмен данными с внешними по отношению к транспортному средству информационными системами через каналы беспроводной связи V2X;
4. специализированному приложению «Автодата»;
5. программному модулю - эмулятору электронных систем и компонентов, включая внутреннюю шину передачи данных, контроллеры, датчики и блоки управления типового транспортного средства, создаваемому в целях отработки требований и технических ращений платформы «Кибербезопасность».

4.3 Требования к обеспечению кибербезопасности внешних систем

В рамках разработки материалов в концепцию платформы «Кибербезопасность» должны быть разработаны функциональные и технические требования и материалы в частное техническое задание на программные модули внешних информационных систем,

являющиеся составными частями платформы «Кибербезопасность» и обеспечивающие защиту данных, получаемых этими системами от транспортных средств, а именно:

- программные модули телематических платформ автопроизводителей, сервис-провайдеров и других участников рынка;
- программные модули дорожного оборудовании V2X и подсистем ИТС (V2X);
- инфраструктуры аутентификаторов;
- подсистемы «Кибербезопасность» Платформы «Автодата».

Должны быть разработаны требования к:

1. функциям программного модуля (программного обеспечения), встраиваемого, либо предусмотренного при разработке, в телематические платформы в целях обеспечения безопасной и некорректируемой передачи данных из транспортных средств в платформу «Автодата»;
2. функциям программного обеспечения, встраиваемого, либо предусмотренного при разработке, в дорожное оборудование V2X и подсистемы ИТС (V2X) в целях защиты и обеспечения некорректируемости данных из транспортных средств в платформу «Автодата»;
3. функциям программного обеспечения инфраструктуры аутентификаторов, обеспечивающей безопасность и конфиденциальность данных как в телематических платформах, оборудовании V2X (бортовом и дорожном), так и подсистемах ИТС (V2X), посредством управления и распределения авторизационных билетов во всех составных частях платформы «Кибербезопасность»;
4. функциям программного обеспечения подсистемы «Кибербезопасность» Платформы «Автодата», обеспечивающего управление процессами загрузки, обновления и настройки специализированного приложения «Автодата», выполняемого на стороне транспортного средства.

Должны быть разработаны функциональные и технические требования к инфраструктуре аутентификаторов, включающей:

1. Корневой центр (КЦ). КЦ должен являться центром высшего уровня в иерархии выдачи аутентификаторов. Он должен предоставлять регистрационному центру и авторизационному центру подтверждение того, что они могут выдавать авторизационные билеты. Центр аутентификаторов должен хранить информацию о своих аутентификаторах и информацию о списках доверия в локальном хранилище.
2. Центр распространения, который должен предоставлять оборудованию V2X и подсистемам ИТС (V2X) актуальные данные, необходимые для выполнения процесса проверки и контроля информации, поступающей от авторизованного оборудования или другого центра аутентификаторов путем публикации перечня действующих аутентификаторов;
3. Регистрационный центр (РЦ). РЦ представляет собой субъект инфраструктуры аутентификаторов, отвечающий за управление жизненным циклом регистрационных данных, а также за проверку взаимной аутентификации оборудования V2X и предоставления доступа к подсистемам ИТС (V2X);

4. Авторизационный центр (АЦ). АЦ - орган управления аутентификаторами, отвечающий за выдачу авторизационных билетов.
5. Авторизационный билет, который должен предоставляться бортовому оборудованию V2X для наделения его полномочиями использовать определенные услуги, предоставляемые дорожным оборудованием V2X и подсистемами ИТС (V2X);
6. Отправляющее оборудование, которое после получения авторизационного билета получает право отправлять сообщения, разрешенные авторизационным билетом.
7. Ретранслирующее оборудование, предназначенное для приема сообщений от отправляющего оборудование и, при необходимости, пересылать их получающему оборудованию.
8. Получающее оборудование – оборудование, получающее сообщения от отправляющего или ретранслирующего оборудования.

Состав и структура инфраструктуры аутентификаторов должны быть уточнены в ходе разработки концепции платформы «Кибербезопасноть» и согласованы с Заказчиком.

5 Состав работ и перечень отчетных материалов

№	Состав работ	Отчетные материалы
1.	Разработка материалов в концепцию платформы «Кибербезопасность» в части требований к защите данных, формируемых электронными системами и компонентами, передаваемых по автомобильной шине передачи данных, их передаче в некорректируемом виде в телематические платформы, требований к телематическим платформам, эксплуатируемым на территории РФ автопроизводителями, сервис-провайдерами, другими участниками рынка, передаче данных из телематических платформ в Платформу «Автодата»	Материалы в концепцию платформы «Кибербезопасность» в части защиты данных на борту транспортного средства, передачи данных в телематические платформы, защиты данных в телематических платформах, защищенной передачи данных в Платформу «Автодата»
2.	Разработка материалов в концепцию платформы «Кибербезопасность» в части разработки: - материалов в частное техническое задание на создание платформы «Кибербезопасность»; - моделей угроз информационной безопасности, включая модели нарушителя	Материалы в ЧТЗ на создание платформы «Кибербезопасность»; Модели угроз информационной безопасности, включая модель нарушителя

3.	Разработка материалов в концепцию платформы «Кибербезопасность» в части требований к защите данных, передаваемых из транспортного средства в подсистемы ИТС (V2X), требований к подсистемам ИТС (V2X) в части защищенной передачи данных в Платформу «Автодата», требований к инфраструктуре аутентификаторов	Материалы в концепцию платформы «Кибербезопасность» в части требований к передаче данных в подсистемы ИТС (V2X), защиты данных в подсистемах ИТС (V2X), защищенной передаче данных в Платформу «Автодата», требований к инфраструктуре аутентификаторов

6 Порядок контроля и приемки системы

Для проведения приемки работ должна быть создана комиссия из представителей Заказчика и Исполнителя.

На приемку результатов работ Исполнитель представляет отчетные материалы.

Приемка работ производится по результатам рассмотрения материалов в концепцию платформы «Кибербезопасность».

По завершении работы комиссии по приемке результатов работ оформляется Акт приемки работ.

На основании акта приемки работ оформляется Акт сдачи-приемки работ.

7 Источники разработки

Для выполнения работ по разработке концепции платформы «Кибербезопасность» Заказчик передает Исполнителю следующую техническую документацию на Платформу «Автодата», разработанную на 2-м этапе проекта:

- Техническое задание на создание Платформы «Автодата»;
- Эскизный проект Платформы «Автодата»;
- Технический проект Платформы «Автодата»;
- ЧТЗ на подсистему защиты информации Платформы «Автодата».

8 Словарь терминов предметной области Системы

Платформа «Автодата» - российская сервисная навигационно-телематическая платформа, обеспечивающая сбор данных из информационных систем различного назначения, относящимся к колесным транспортным средствам, дорожной инфраструктуре, иной информации автотранспортной сферы, в том числе связанной с логистикой людей и вещей, обработку и обогащение собранных данных, формирование статистики и аналитики, предоставление сервисов и информационных продуктов широкому кругу потребителей.

8.1.1 **Описание предметной области**

Предметная область Системы представляет собой совокупность процессов и сущностей автотранспортной и дорожно-транспортной сферы. Основными сущностями предметной области Системы являются следующие:

- транспортное средство;
- дорога (участок дороги);
- дорожно-транспортная инфраструктура.

В процессе взаимодействия между сущностями «транспортное средство», «дорога» и «дорожно-транспортная инфраструктура» возникают отношения, которые образуют сущность «дорожное движение».

Основные сущности предметной области представлены на рисунке далее (Рисунок 1).

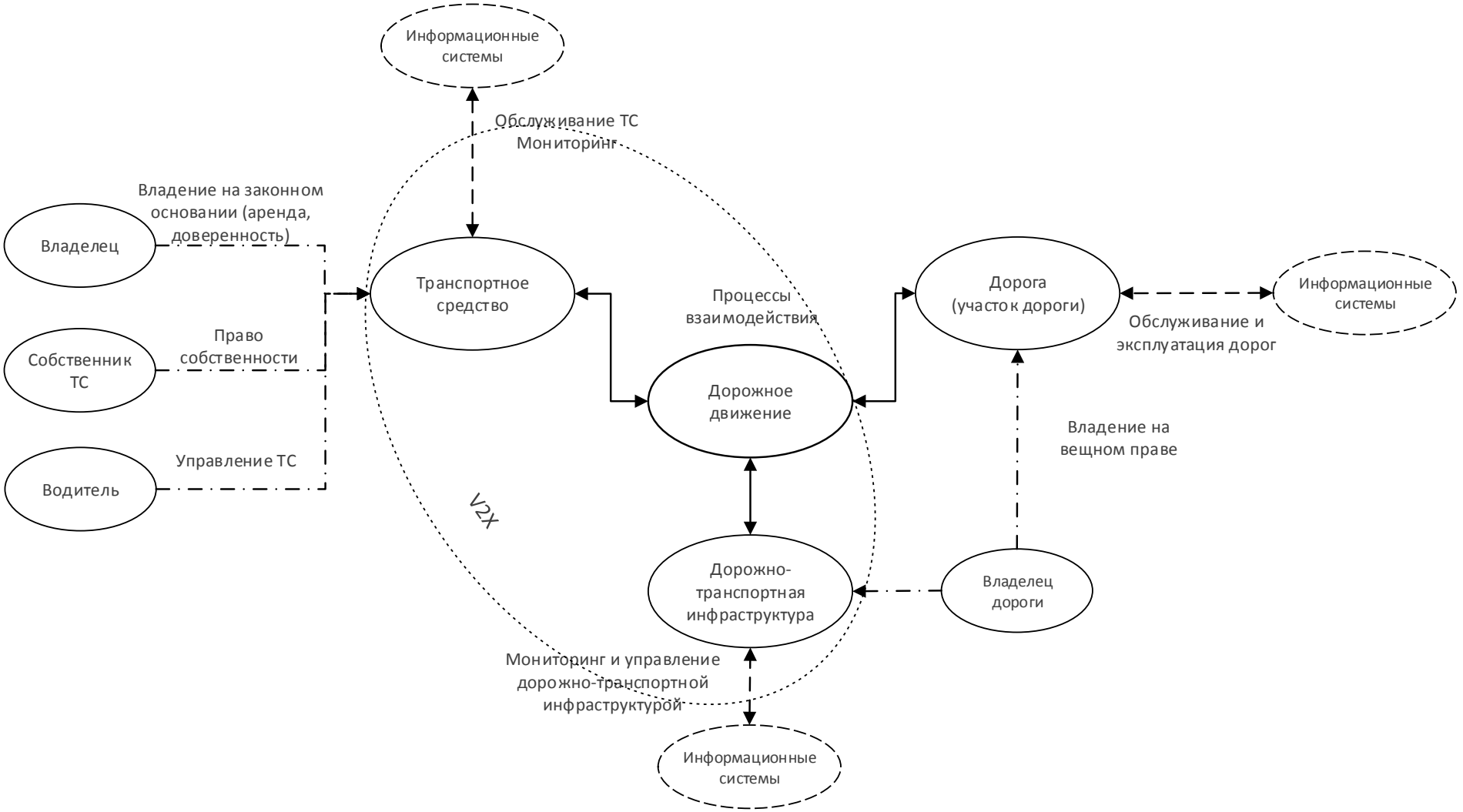

Рисунок 1 – Основные сущности предметной области

Сущность «транспортное средство» описывает основные технические и эксплуатационные характеристики транспортного средства. Классификация транспортных средств определяется Техническим регламентом Таможенного союза «О безопасности колёсных транспортных средств», который вводит понятия категорий транспортных средств. Технический регламент определяет следующие категории транспортных средств:

- Категория L - мототранспортные средства. В данную категорию включаются мопеды, мотовелосипеды, мокики;
- Категория M - пассажирские транспортные средства. В данную категорию включаются легковые автомобили, автобусы, троллейбусы;
- Категория N - грузовые автомобили. В данную категорию включаются грузовые автомобили;
- Категория O – прицепы.

Технический регламент определяет понятия специальных и специализированных транспортных средств. К специальным транспортным средствам относятся: автокраны, пожарные автомобили, автомобили, оснащенные подъемниками с рабочими платформами, автоэвакуаторы, коммунальная техника и т.д. К специализированным относятся транспортные средства, предназначенные для перевозки нефтепродуктов, пищевых жидкостей, сжиженных углеводородных газов и т.д.

С сущностью «транспортное средство» связаны следующие сущности, имеющие непосредственное отношение к транспортному средству:

- Собственник транспортного средства - физическое или юридическое лицо, владеющий транспортным средством по праву собственности;
- Владелец транспортного средства - физическое или юридическое лицо, владеющий транспортным средством по вещному праву (аренда, доверенность), обеспечивающий эксплуатацию и обслуживание транспортного средства;
- Водитель транспортного средства - физическое лицо, управляющее транспортным средством.

Сущность «дорожно-транспортная инфраструктура» описывает основные группы и типы объектов дорожно-транспортной инфраструктуры и их характеристики. Объекты дорожно-транспортной инфраструктуры располагаются на участках дорог и имеют привязку к сущности «дорога».

Классификация объектов дорожно-транспортной инфраструктуры определена в ГОСТ 32846-2014 «Дороги автомобильные общего пользования. Элементы обустройства. Классификация» и включает в себя следующие группы и типы объектов дорожно-транспортной инфраструктуры:

- объекты обслуживания участников дорожного движения: автостоянка, парковка, устройство аварийно-вызывной связи и другие;
- объекты контроля за движением: автоматизированные датчики погодных условий, пункт весового и габаритного контроля, пункт контроля международных автомобильных перевозок, пункт взимания платы за проезд, автоматизированный счетчик учета интенсивности движения, технические средства для информирования, зрительного ориентирования участников дорожного движения и регулирования движения: дорожный знак, дорожный знак переменной информации, дорожная разметка, дорожный светофор;

- защитные устройства: дорожное заграждение, дорожное ограждение, акустический экран, противоослепляющий экран;
- средства улучшения условий видимости: дорожное зеркало, постоянное стационарное электрическое освещение;
- снегозащитные устройства и насаждения, противогололедные устройства: снегозащитные насаждения, оборудование для борьбы с зимней скользкостью, снегозащитное устройство.

В состав дорожно-транспортной инфраструктуры входит интеллектуальная транспортная система (ИТС), предназначенная для автоматизированного исполнения максимально эффективных сценариев управления транспортно-дорожным комплексом с целью максимизации показателей использования дорожной сети, повышения безопасности и эффективности транспортного процесса, комфортности для водителей и пользователей транспорта. Составной частью ИТС являются подсистемы ИТС (V2X) и бортовое (OBU) и дорожное (RSU) оборудование V2X, обеспечивающие беспроводную передачу данных автомобилей между собой и между автомобилями и дорожным оборудованием, а также подсистемами ИТС (V2X).

К объектам дорожно-транспортной инфраструктуры также относят камеры фотовидеофиксации и дорожные оборудование V2X (RSU - Road Side Unit).

Между транспортными средствами, оснащенными бортовым оборудованием V2X (OBU - onboard unit) и между транспортными средствами и дорожным оборудованием (RSU) возникает информационное взаимодействие, позволяющее транспортным средствам осуществлять помощь водителям (в дальнейшем самостоятельно принимать решения) в принятии решений в различных транспортных ситуациях.

Сущность «дорога» описывает основные технические, эксплуатационные и географические характеристики участков дорог.

В соответствии с федеральным законом № 257 от 8.11.2007 г. «Об автомобильных дорогах и о дорожной деятельности в Российской федерации» принята следующая классификация дорог:

- автомобильные дороги федерального значения;
- автомобильные дороги регионального или межмуниципального значения;
- автомобильные дороги местного значения;
- частные автомобильные дороги.

Автомобильные дороги общего пользования в зависимости от условий проезда по ним и доступа на них транспортных средств подразделяются на:

- автомагистрали;
- скоростные автомобильные дороги;
- обычные автомобильные дороги.

С сущностями «дорожно-транспортная инфраструктура» и «дорога» связана сущность «владелец дороги». Владельцы автомобильных дорог обеспечивают эксплуатацию и обслуживание участков дорог и установленной на них дорожно-транспортной инфраструктуры, включая мониторинг состояния дорожного покрытия и состояние оборудования, организацию проведения ремонтных работ и замену вышедшего из строя оборудования.

Сущность «дорожное движение» описывает процесс взаимодействия между транспортными средствами, дорогой и объектами дорожно-транспортной инфраструктуры.

В результате взаимодействия образуется массив информации характеризующий местоположение транспортных средств, параметры их движения, аварийные ситуации, дорожно-транспортные происшествия, нарушения правил дорожного движения, грузо- и пассажироперевозки, нарушения установленных норм и правил.

Сущность «Информационные системы» опосредовано связана с основными сущностями «транспортное средство», «дорожно-транспортная инфраструктура», «дорога» и «дорожное движение» и обеспечивают сбор информации об объектах основных сущностей, ее обработку и решение широкого круга задач мониторинга и эффективного управления. Информационные системы, использующиеся в автотранспортной и дорожно-транспортной сфере, классифицируются по признаку владения и по типу решаемых задач. По признаку владения информационные системы классифицируются на следующие виды:

- государственные информационные системы (ГИС, ГИАС);
- подведомственные информационные системы;
- информационные системы коммерческих участников рынка.

По типу решаемых задач информационные системы, использующиеся в автотранспортной и дорожно-транспортной сфере, классифицируются на следующие виды:

- предназначенные для обеспечения контрольно-надзорных функций на основе информации, получаемой от транспортных средств, объектов дорожно-транспортной инфраструктуры;
- предназначенные для обеспечения мониторинга и управления объектами;
- предназначенные для обеспечения аналитических функций и функций поддержки принятия решений;
- предназначенные для предоставления услуг на основе информации, получаемой от транспортных средств, объектов дорожно-транспортной инфраструктуры и ее обработки.

8.1.2 **Термины и определения**

Термин	**Определение**
Автомобильная система V2X (OBU), бортовое оборудование V2X	Бортовое оборудование, обеспечивающее обмен данными между транспортными средствами, транспортными средствами и элементами дорожной инфраструктуры, сетями подвижной радиотелефонной связи в различных сценариях обеспечения безопасности и управления дорожным движением интеллектуальных транспортных систем (ИТС), работающее на основе технологий ближнего радиуса действия в частотном диапазоне 5,8 – 5,9 ГГц, соответствующее Европейскому стандарту ITS-G5 и международным стандартам IEEE 802.11p и IEEE 1609, либо C-V2X в соответствии со стандартами 3GPP
Бортовое телематическое оборудование	Обобщённое название аппаратуры спутниковой навигации (АСН), а также штатного и дополнительного бортового оборудования, обладающих функциональными возможностями взаимодействия со штатными или

	дополнительно устанавливаемыми электронными системами ТС и позволяющие определить текущее местоположение ТС, а также направление и скорость его движения (по сигналам не менее двух действующих глобальных навигационных спутниковых систем), а также используемых для приема и передачи информации посредством сетей подвижной радиотелефонной связи, сетей ведомственной связи и (или) систем беспроводной связи ближнего радиуса действия информацией
Дорожное оборудование V2X (RSU - Road Side Unit)	Дорожное оборудование, обеспечивающее обмен данными между элементами дорожной инфраструктуры и транспортными средствами, сетями подвижной радиотелефонной связи в различных сценариях обеспечения безопасности и управления дорожным движением интеллектуальных транспортных систем (ИТС), работающее на основе технологий ближнего радиуса действия в частотном диапазоне 5,8 – 5,9 ГГц, соответствующее Европейскому стандарту ITS-G5 и международным стандартам IEEE 802.11p и IEEE 1609, либо C-V2X в соответствии со стандартами 3GPP
Интеллектуальная транспортная система (ИТС)	Система управления, интегрирующая современные информационные и телематические технологии и предназначенная для автоматизированного поиска и принятия к реализации максимально эффективных сценариев управления транспортно-дорожным комплексом региона, конкретным транспортным средством или группой ТС с целью обеспечения заданной мобильности населения, максимизации показателей использования дорожной сети, повышения безопасности и эффективности транспортного процесса, комфортности для водителей и пользователей транспорта
Инфраструктура аутентификаторов	Многоуровневая система центров управления аутентификаторами (создание, проверка, подтверждение владения, проверка срока действия, аннулирование, выдача, ведение реестра выданных и аннулированных аутентификаторов) и авторизационными билетами и билетами проверки авторизации (создание, проверка уникальности) и т.д.
Платформа «Автодата»	Российская сервисная навигационно-телематическая платформа, обеспечивающая сбор данных из информационных систем различного назначения, относящимся к колесным транспортным средствам, дорожной инфраструктуре, иной информации автотранспортной сферы, в том числе связанной с логистикой людей и вещей, обработку

	и обогащение собранных данных, формирование статистики и аналитики, предоставление сервисов и информационных продуктов широкому кругу потребителей
Платформа «Кибербезопасность»	Совокупность программ для ЭВМ, обеспечивающих защиту и безопасность данных, формируемых в электронных системах и компонентах автомобиля и передаваемых посредством автомобильного бортового телематического оборудования и бортового оборудования V2X через беспроводные сети и каналы связи в телематические платформы автопроизводителей и других участников рынка и подсистемы ИТС (V2X) в целях их дальнейшего предоставления в платформу «Автодата»
AUTOSAR	AUTomotive Open System ARchitecture (AUTOSAR) – международное партнерство автопроизводителей, поставщиков автомобильной электроники, сервис-провайдеров, производителей программного обеспечения и микроэлектроники по разработке и стандартизации архитектуры автомобильного программного обеспечения
Платформа AUTOSAR Adaptive	Перспективный подход, требования и стандарты разработки программного обеспечения электронных систем и компонентов транспортного средства, включающий использование сервисно-ориентированней архитектуры и средств виртуализации, обеспечивающий гибкость разработки приложений, информационную безопасность, управление конфигурациями, настройками и защищенным обменом данных между транспортными средствами и внешними информационными системами, в том числе для загрузки и обновления прикладного и системного программного обеспечения (https://www.autosar.org/standards/adaptive-platform/).
Подсистемы ИТС (V2X)	Комплексные подсистемы ИТС, программно-аппаратные комплексы, предназначенные для сбора, обработки и хранения данных от бортового оборудования V2X (OBU), оборудования V2X дорожной инфраструктуры (RSU) и предоставление пользователям различных сервисов, направленных на обеспечение безопасности дорожного движения, оптимизацию дорожного движения и др.
Телематическая платформа	Аппаратно-программный комплекс, предназначенный для сбора, обработки, хранения и маршрутизации навигационных, телематических, технологических и других данных от бортового телематического оборудования транспортного

	средства в информационные системы различного назначения, а также обмена данными между информационными системами и бортовым телематическим оборудованием
Транспортное средство	Устройство на колесном ходу категорий L, M, N, T (по ГОСТ Р 52051-2003), в том числе специального назначения (C) и повышенной проходимости (G), предназначенное для перевозки людей, грузов или оборудования, установленного на нем (Технический регламент Таможенного союза ТР ТС 018/2011 «О безопасности колёсных транспортных средств»), а также прочих транспортных и технологических операций
V2X	См. Автомобильная система V2x.

СОСТАВИЛИ

Наименование организации, предприятия	**Должность исполнителя**	**Фамилия, имя, отчество**	**Подпись**	**Дата**

СОГЛАСОВАНО

Наименование организации, предприятия	**Должность исполнителя**	**Фамилия, имя, отчество**	**Подпись**	**Дата**