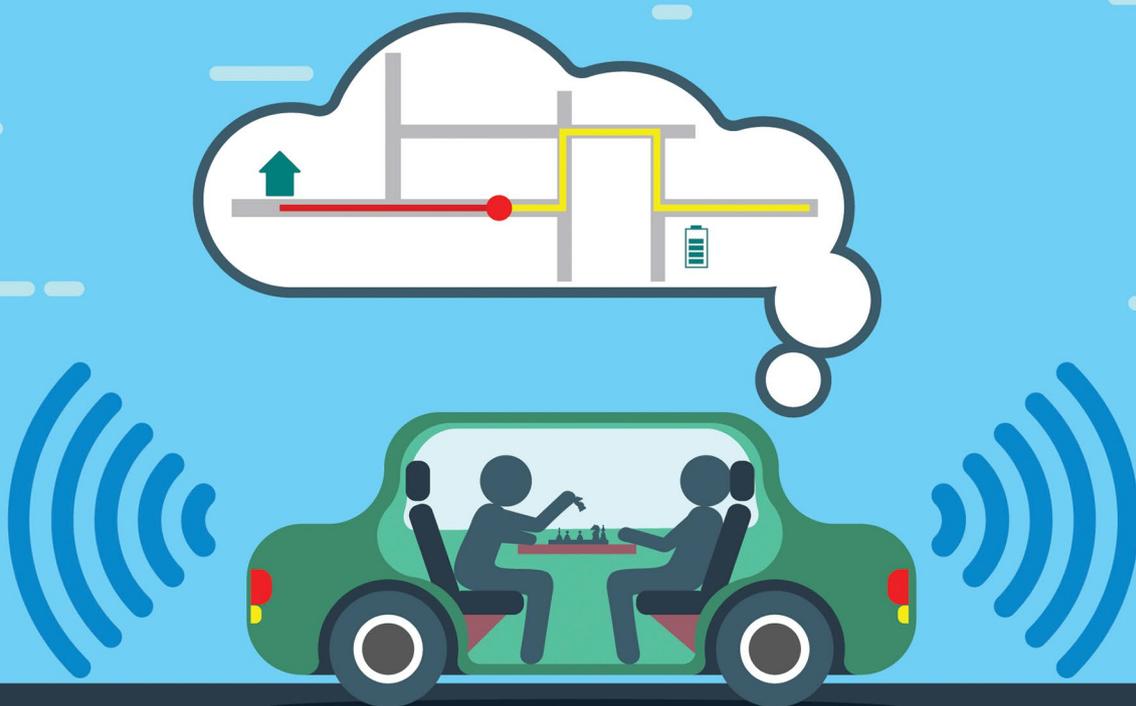


Дорожная инфраструктура и высокоавтоматизированные транспортные средства

DOI: 10.17273/CADGIS.2019.2.7

Евстигнеев И.А., начальник отдела перспективных систем департамента информационных технологий и интеллектуальных транспортных систем Государственной компании «Автодор» (г. Москва)

Рассматривается неоднозначная трактовка понятия цифровой телекоммуникационной инфраструктуры. Анализируются условия внедрения высокоавтоматизированных транспортных средств в дорожную инфраструктуру. Описываются основные технологические проблемы дорожной телекоммуникационной инфраструктуры, которые необходимо решить для обеспечения безопасного движения высокоавтоматизированных транспортных средств, а также даются рекомендации по их устранению.



К вопросу терминологии

Готова ли инфраструктура городов и федеральных дорог к массовому использованию высокоавтоматизированных транспортных средств (ВАТС)? Давайте поразмышляем именно в области технических рисков.

К сожалению, пока понятие цифровой телекоммуникационной инфраструктуры, обеспечивающей ВАТС необходимыми сервисами и информацией, является неоднозначным.

Под цифровой инфраструктурой часто понимают цифровую копию (модель) физической инфраструктуры. Применительно к наземному транспорту это в основном высокоточные трёхмерные цифровые карты. В литературе сейчас одновременно встречаются также понятия «информационная инфраструктура», «интеллектуальная инфраструктура», «инфраструктура цифровой экономики», «умная инфраструктура» и другие похожие термины. В целом под цифровой инфраструктурой понимается скорее информационно-коммуникационная инфраструктура как совокупность средств передачи, хранения, обработки и представления информации, предназначенная для повышения эффективности работы некоторой системы в целом.

В более широком контексте цифровая инфраструктура понимается уже как совокупность социально-технических систем, включающая влияние разработчиков и пользователей информационных технологий.

В материалах Европейской комиссии понятие цифровой инфраструктуры обозначается так: «Статическое и динамическое цифровое отображение физического мира, с которым автоматизированные транспортные средства будут взаимодействовать в процессе эксплуатации. Сюда входят сбор, обработка и передача информации».

Так что термин «цифровая инфраструктура», хотя он и получил широкое распространение, носит скорее обобщающий характер, чем является научно-техническим определением.

Условия внедрения ВАТС в дорожную инфраструктуру

По мнению автора, начальный этап внедрения ВАТС, а возможно и дальнейшие этапы, однозначно потребует поддержки со стороны дорожной инфраструктуры. Не исключено, что при дальнейшем развитии технологий ВАТС, вероятно, смогут создаваться без особых требований к оснащению дороги.

Скорее предпочтителен «гибридный» подход, основанный на использовании нескольких технологий для обеспечения наилучшей функциональности системы «транспортное средство + инфраструктура», однако их наиболее эффективное сочетание всё ещё не найдено.

Развитие ВАТС нельзя рассматривать изолированно от коммуникационных систем, обеспечивающих «подключённость» автомобилей. Все

передовые разработки по реальному внедрению ВАТС ведутся как минимум с учётом возможностей «подключённости», а в большинстве своём непосредственно на основе таких технологий.

Без интеллектуальной инфраструктуры, которая способна принять на себя часть задач, стоящих перед ВАТС, цена таких автомобилей может стать неприемлемой для коммерческого использования.

Успешное функционирование ВАТС зависит от большого количества датчиков, лидаров, радаров, камер и т.д., и все эти элементы увеличивают стоимость производства транспортных средств. Мало того, все они имеют серьёзные недостатки и технические ограничения.

- Проблемы видеокамер: ограниченная зона видимости для полноценного обзора, дорожная грязь, снег, низко сидящее яркое солнце, проблесковая реклама на улично-дорожной сети города.
- Проблемы лидаров: крайне высокая стоимость (40–70 тысяч долларов), сложность подбора алгоритмического компромисса по выявлению опасных для движения объектов.
- Проблемы радаров: выдают мало доступной информации.

Без интеллектуальной инфраструктуры, которая способна принять на себя часть задач, стоящих перед ВАТС, цена таких автомобилей может стать неприемлемой для коммерческого использования.

Одним из способов уменьшения стоимости ВАТС является перераспределение ответственности, сконцентрированной в данный момент на транспортном средстве, на систему, включающую транспортное средство и инфраструктуру. При развёртывании на ограниченных участках (когда не надо сразу оснастить целый город) вполне вероятно, что подобная система окажется более экономичной, чем дорогой полный набор сенсоров в транспортном средстве.

Взаимодействие с инфраструктурой открывает новые возможности в управлении транспортными потоками и значительный потенциал в повышении эффективности дорожного движения, что также говорит об очевидной необходимости внедрения этих технологий. В этом случае автоматизация не только поддерживается инфраструктурой, но и фактически ею обеспечивается.

Все участвующие в движении автомобили должны быть оснащены оборудованием V2V, V2I, V2X и т.п. При таком подходе автоматизация может предоставляться как услуга (подобно проезду по платному участку дороги), а пользователи будут платить за неё по мере необходимости.

Компетенции и обязанности по организации автоматизированного управления транспортным средством (ТС) разделяются между инфраструктурой (которая будет обеспечивать ситуационную осведомлённость), сторонними поставщиками программного обеспечения, встроенного в ТС (и принимающего решения по управлению), и традиционными OEM-производителями автомобилей (которые предоставляют сами машины, оснащённые двигательными установками и иными необходимыми элементами).

Коммуникация ТС с инфраструктурой будет стимулировать развитие интеллектуальных городов, где сочетание современных методов организации дорожного движения, «умной парковки» и административных воздействий приведёт к улучшению общей дорожной ситуации и повысит её безопасность. Связь транспортных средств с инфраструктурой поможет во время аварий и чрезвычайных ситуаций и будет значительным достижением на пути к полной автоматизации.

Несмотря на стремительный прогресс, ещё остаются нерешённые технологические проблемы, которые препятствуют повсеместному распространению ВАТС, в том числе в сфере формирования дорожной инфраструктуры.

Основные технологические проблемы (факторы риска) дорожной инфотелекоммуникационной инфраструктуры для обеспечения движения ВАТС

1. Необходимость получения, хранения и обработки больших данных в режиме реального времени

Текущие риски

- Объём данных, генерируемых объектами транспортной системы, уже достаточно велик и, как ожидается, будет быстро расти. При большом скоплении связанных автомобилей имеет место лавинообразное нарастание количества исходных данных для анализа, что приводит к ошибкам и медлительности работы бортовых устройств.
- Необходимость безопасного и эффективного управления ВАТС в режиме жёсткого реального времени.
- Отсутствие либо низкий уровень интеллектуальности систем управления ВАТС на современном этапе развития, исключающий возможность их использования в условиях сложной и динамически изменяющейся дорожной обстановки.
- Отсутствие единых правил, которые опишут, как обращаться с данными, кто ими владеет, можно ли и по какой цене эти данные купить.
- Владельцам данных может не понравиться идея отдавать свои данные в чужую систему,

при этом что зарабатывать на них будут не они сами, а, возможно, их конкурент.

Рекомендации

Безусловно, в современном мире данные — один из важнейших активов.

Технология больших данных подразумевает наличие трёх элементов: огромных массивов данных, вычислительных мощностей для очень быстрой обработки этих данных и специальных математических моделей, позволяющих сравнивать заранее определённые параметры, доступ к которым раньше был запрещён. Это позволяет выявлять новые, очень часто неочевидные связи и закономерности и уже на их основе принимать управленческие решения и извлекать прибыль.

На сегодняшний день участники российского и зарубежного рынков создали межотраслевой консорциум «Автодата.Рус». Планируется, что консорциум создаст национальную сервисную телематическую платформу «Автодата», которая будет аккумулировать данные по автомобилям¹.

На базе платформы предполагается создание сервисов, включая макеты «умной автомобильной магистрали», «умной дорожной сети». Пока это совершенно неурегулированное поле деятельности. Соответственно, дать отрицательную или положительную рекомендацию деятельности проекта «Автодата» невозможно, всё будет зависеть от того, как оперативно и грамотно будут решены текущие проблемы в области больших данных, но в любом случае данное стремление нужно считать положительным фактором.

2. Системы связи V2X (автомобиль — автомобиль, автомобиль — инфраструктура, автомобиль — другие участники движения)

Текущие риски

- Отсутствие устойчивого покрытия автодорог сетью 4G.
- Теоретически сеть стандарта 5G позволит автомобилям взаимодействовать с диспетчерской службой и между собой в режиме реального времени и без задержек, присущих существующим сотовым сетям. Это действительно важно. Для качественного покрытия и высокой надёжности базовые станции придётся установить очень часто. Это огромные вложения в инфраструктуру.
- Серьёзные проблемы выделения и расчёта частот для сетей 5G. Реализация программы «цифровой экономики» буксует из-за того, что оборонное ведомство не хочет отдавать подходящие частоты. Минобороны РФ выступило против передачи операторам мобильной связи частот в диапазоне 3,4–3,8 ГГц. Министерство обороны РФ предложило использовать для 5G частоты в диапазонах 4,8–4,99 ГГц и 27,1–27,5 ГГц, ра-

¹ <https://www.comnews.ru/content/122298/2019-10-01/avtodatarus-krupnyeshee-hranilishche-dannyh-v-mire>

нее одобренные Госкомиссией по радиочастотам. Однако под первый диапазон в России попросту нет коммерческого оборудования, а второй подходит лишь для локального покрытия. Диапазон 3,4–3,8 ГГц, который в наибольшей степени подходит для 5G, занят средствами спутниковой связи Минобороны и других силовых ведомств.

- Фактически требуется создание системы гарантированной связи на расстояниях до 200 м и относительных скоростях до 120 м/с уровня не ниже ASIL B ISO 26262, степени защиты не ниже IP45 ГОСТ 14254-96 и латентностью не более 1 мс.

Элементы дорожной инфраструктуры кооперативных систем, обеспечивающих информирование водителя, должны обеспечивать непрерывную передачу данных между транспортными средствами и дорожной инфраструктурой.

Технологическое обеспечение систем связи (передатчики, приёмники, каналы, протоколы, конфигурации сетей и т.п.) играет в данном контексте уже второстепенную роль. Основное требование к системам связи — это надёжная и быстрая передача требуемого объёма данных. Какими техническими средствами это достигается — не так важно при рассмотрении систем управления.

Рекомендации

Необходимо развитие технологий беспроводной передачи данных для обеспечения максимально быстрого (мгновенного) обмена информацией автомобилями высокой степени автономности между собой и с объектами инфраструктуры.

Естественно, основными местами размещения радиоэлектронных средств являются крупные города и примыкающие к ним территории. Следствием этого является сложная электромагнитная обстановка на данных территориях и фактически отсутствие свободного радиочастотного ресурса. Предстоит серьёзная борьба между владельцами частотного ресурса не только в России, но и по всему миру.

На территории Российской Федерации отсутствуют стандарты на подобные системы связи. При этом существуют значительные трудности по

Основное требование к системам связи — это надёжная и быстрая передача требуемого объёма данных. Какими техническими средствами это достигается — не так важно при рассмотрении систем управления.

внедрению таких систем, т.к. остаются нерешёнными вопросы электромагнитной совместимости.

3. Картография, ГИС, навигация

Текущие риски

- Отсутствие решений, как поддерживать актуальность высокоточных цифровых карт.
- Отсутствие понимания в унификации цифровых карт.

Большинство водителей уже сталкивались с неактуальными картами в навигаторе, когда на дороге проводился ремонт, случилось дорожно-транспортное происшествие или недавно построили новую развязку. А как быть ВАТС?

Большой риск — отсутствие в достаточном объёме картографического обеспечения, описывающего дорожную инфраструктуру с достаточной для движения ВАТС точностью (до сантиметров в плане), а также отсутствие системы внесения изменений в картографическое обеспечение для участков дорожной сети с высокой динамикой изменений элементов окружающей среды.

Пока приходится ориентироваться на различные неунифицированные HD maps (high definition maps) — карты, построенные с высоким разрешением.

Рекомендации

С целью повышения безопасности дорожного движения высоко- и полностью автоматизированных (беспилотных) транспортных средств, а также повышения мобильности и комфорта для участников дорожного движения необходима разработка и внедрение цифровой модели дороги (ЦМД), основанной на достоверных высокоточных пространственных данных о дороге и условиях движения. ЦМД необходимо разработать для всех дорог, предназначенных для применения ВАТС.

Для ЦМД допускается применение различных карт, прошедших соответствующую сертификацию на предмет унификации объектов отображения,

надёжности, качества, достоверности и своевременности обновления.

Дорожно-транспортная инфраструктура должна обладать возможностью обеспечить передачу с заданными параметрами качества управляющих воздействий и данных о ситуационной осведомлённости, а также своевременное обновление дорожной карты на участке дороги, по которому следует ВАТС.

ЦМД должна обеспечивать:

- ситуационную осведомлённость ВАТС;
- оптимальное перераспределение транспортных потоков ВАТС для достижения заданных показателей качества обслуживания различных клиентских групп;
- управление ВАТС в различных нештатных ситуациях;
- решение конфликтных ситуаций на стратегическом уровне управления транспортными потоками ВАТС;
- поддержку реализации автоматической системы управления дорожным движением для ВАТС, эксплуатирующихся в беспилотном режиме;
- удалённый доступ пользователей ВАТС к пользовательским сервисам ЦМД в онлайн- и офлайн-режимах.

ЦМД должна содержать:

- цифровую крупномасштабную навигационную карту с описанием структурных линий дорог, дорожной разметки, дорожных знаков, светофоров и т.п.;
- цифровой граф дорог;
- цифровые сведения об условиях движения, характеризующие текущую дорожно-транспортную обстановку (препятствия, аварии, плохие погодные условия, низкое качество дорожного покрытия и пр.);
- данные, описывающие объекты придорожной инфраструктуры и сервиса;
- слои обработки исходной информации и формирования управля-

ющих воздействий на транспортный поток ВАТС;

- интерфейс взаимодействия с интеллектуальными транспортными системами (ИТС) (кооперативными ИТС);
- аппаратно-программный комплекс реализации пользовательских сервисов.

При формировании высокоточных цифровых динамических карт предлагается руководствоваться основными международными телекоммуникационными стандартами в области интеллектуальных транспортных систем:

- ISO/PRF TR 17424 — Intelligent transport systems — Cooperative systems — State of the art of Local Dynamic Maps concepts;
- ISO/PRF TS 18750 — Intelligent transport systems — Cooperative systems — Definition of a global concept for Local Dynamic Maps;

а также другими решениями уполномоченных органов (в том числе международных) в данной области.

4. Системы глобального и локального позиционирования. Технологии повышения точности навигации

Текущие риски

Практически все ВАТС используют GPS/ГЛОНАСС, глобальную спутниковую систему навигации, и от неё нельзя отказаться.

С высокой степенью вероятности может потребоваться дополнительное оборудование дороги устройствами, обеспечивающими высокоточное позиционирование ВАТС (например, сервисом дифференциальных поправок GPS/ГЛОНАСС — RTK, «кинематикой реального времени»).

Однако что произойдёт с ВАТС, если пропадёт сигнал от спутника? Оно просто остановится посередине оживлённого перекрёстка...

Рекомендации

С целью повышения безопасности дорожного движения автотранспортных средств (в том числе беспилотных), достижения мобильности и комфорта для участников дорожного движения сформировать в составе дорожной инфраструктуры систему высокоточного позиционирования дороги (СВПД) на основе методов определения местоположения объектов по

Для реализации даже простейших сценариев необходимо, чтобы минимум 10% автопарка было оснащено беспроводными модулями, а оптимальная доля — это порядка 80%.

сигналам глобальных спутниковых навигационных систем.

Возможным вариантом состава СВПД является:

- линейная сеть референчных базовых станций;
- сетевой центр управления;
- волоконно-оптическая линия связи;
- канал мобильной радиосвязи.

СВПД должна обеспечивать:

- сбор, хранение, обработку информации от базовых станций, выработку и выдачу на приёмник пользователя корректирующей информации;
- точность определения местоположения движущегося автотранспортного средства в режиме реального времени не хуже 0,10 м в плане;
- периодичность определения местоположения автотранспортного средства (с частотой, обеспечивающей требуемый функционал).

5. Несовершенство искусственного интеллекта. Видеодетекция, транспортная аналитика и автоматический контроль движения

Текущие риски

- Отсутствие решений для адаптации элементов инфраструктуры к переходному периоду при одновременном движении в потоке обычных транспортных средств (с ручным управлением) и ВАТС. Для реализации даже простейших сценариев необходимо, чтобы минимум 10% автопарка было оснащено беспроводными модулями, а оптимальная доля — это порядка 80%. Простые расчёты показывают, что, если человечество будет устанавливать на все без исключения новые автомобили данные системы, на достижение 10-процентного барьера уйдёт порядка двух лет. В реальности, конечно, срок будет значительно больше.
- Также ситуацию омрачают перемещающиеся по той же дороге «непродвинутые» мотоциклисты,

обладатели мопедов, конных повозок и велосипедов.

- Отсутствие надёжных решений для систем информирования ВАТС о ситуации на дорожной сети. ВАТС может вести себя малопредсказуемо при некоторых цветовых сочетаниях, фактически постоянно путаясь в оценке образа объекта. Скорее всего, потребуются дополнительные элементы дорожной инфраструктуры для мониторинга погодных условий, состояния дорожного покрытия и т.д.
- Отсутствие надёжных алгоритмов обработки и сопоставления информации в реальном времени. Сегодня искусственному интеллекту очень тяжело понять, какие объекты нужно анализировать, а какие отбросить. Фактически требуется распознавание объектов в режиме реального времени (не более 10 мс) на процессорах с низким потреблением энергии и точностью 99,9%.
- Высокие требования к вычислительной мощности. Современные алгоритмы обработки изображений постоянно только повышают требования к вычислительным мощностям.
- Системы принятия решений уровня ASIL D ISO 26262.

Рекомендации

Выход только один — закладывание алгоритмов видеообработки, позволяющих быть устойчивым к таким видам рисков.

6. Отсутствие отработанных конструктивных решений для развёртывания элементов цифровой дорожной инфраструктуры, необходимых для эффективного использования ВАТС

Текущие риски

- Критически важным аспектом, связанным с развитием технологий автономного вождения, является способность таких ав-

тономных систем эффективно и безопасно взаимодействовать с окружающей транспортной инфраструктурой в различных дорожных ситуациях (например, взаимодействовать с различными типами пользователей, неожиданными препятствиями) вне зависимости от внешних условий (например, плохих погодных условий или плохой видимости).

- Пока можно констатировать факт, что большинство производителей ВАС в настоящее время не уделяют значительного внимания вопросу кооперативного управления ВАС. Их основные усилия направлены на разработку алгоритмов движения индивидуальных ВАС в широком спектре режимов и дорожных ситуаций, поскольку основная задача — это как можно скорее выпустить продукт, привлекательный для конечного пользователя. Увы, но в основном за счёт экономии на безопасности дорожного движения.

Рекомендации

Целесообразно применение механизмов государственно-частного партнёрства или приватизация государственных участков или объектов дорожной инфраструктуры, которые потребуют модернизации (оснащения необходимым оборудованием сервиса безопасности (автомобиль — инфраструктура)) и адаптации дорожного полотна, разметки, знаков и парковочных мест для эксплуатации транспортных средств различного уровня автономности.

Вслед за закреплением обязанности оснащать на территории Европейского союза все транспортные средства современными системами помощи водителю, такими как АЕBS (правила Европейского союза 347/2012, 2015/562) и LDW

(правило Европейского союза 351/2012), ужесточение требований по безопасности закономерно потребует обеспечения возможности взаимодействия со светофорами, дорожными знаками, другими участниками движения для получения новой и дополнительной информации.

Основным направлением стимулирования развития инфраструктуры для беспилотного транспорта и интеллектуальных транспортных систем является разработка типовых моделей и выработка требований (рекомендаций) к оснащению транспортных средств и инфраструктуры информационно-телекоммуникационными средствами автомобильного и городского электрического транспорта для различных территорий, принятие соответствующих нормативных (рекомендательных) документов, в том числе по порядку и срокам оснащения.

7. Приватность.

Конфиденциальность персональных данных пользователей и кибербезопасность (хакерские атаки, компьютерные взломы и вирусы)

Текущие риски

- Фактически существует крайне слабая защита личных данных человека в современном мире. Возможность получить личные данные (легально или нелегально) почти любого человека — это реалии современного мира. ВАС постоянно фиксирует всю информацию о своих перемещениях: маршрут, время поездки, места остановок. Пока не сняты опасения, что злоумышленники могут получить данные с помощью технологий кооперативных ИТС о перемещении конкретных физических лиц (водителей).



- Не проработаны решения в части изучения влияния помех (например, нелицензированных Wi-Fi-устройств) на работу кооперативных ИТС.
- Растёт вероятность того, что соединённые с интернетом автомобили могут не только нанести ущерб пассажирам или пешеходам, но однажды могут быть массово выведены из строя.

Рекомендации

Рекомендуется использовать комплексное сочетание технологий и систем в области безопасности, в том числе базовые программные или программно-аппаратные системы защиты, шифрование данных и биометрические данные (отпечаток пальца, распознавание голоса, лица и иные), чтобы помочь физически аутентифицировать пользователей транспортных средств.

Использование множества разных сетей для подключения автомобилей к интернету позволит уменьшить количество машин, которое злоумышленники смогут вывести из строя с помощью единичного взлома. Если, скажем, не больше пяти процентов ВАТС будут объединены одной сетью или будут использовать одни и те же сетевые протоколы, то риск пробок, парализующих весь город, будет низким. Следовательно, хакер, задумавший вызвать серьёзные проблемы, столкнётся с раздроблённой многосетевой архитектурой и будет вынужден осуществить множество одновременных взломов. Это повышает сложность атаки и делает её менее вероятной.

Следует убедиться, что ВАТС надёжно защищены от попыток радиоэлектронного подавления, перехвата управления и утечки передаваемой информации, включая персональные данные пользователей. Необходимо выполнять системное проектирование ВАТС с учётом минимизации рисков для безопасности из-за кибернетических угроз и уязвимостей ПО. Решения, касающиеся кибербезопасности, должны интегрироваться в систему управления ТС на этапах его разработки.

Рекомендуется осуществлять обеспечение кибербезопасности не только за счёт дополнительных систем защиты, но и на основе максимального исключения принципиальной возможности вмешательства (Safe by Design Concept), физической невозможности управления движением извне, например передачи дистанционного управления внешнему оператору только посредством ручного переключателя.

Отчёт о кибербезопасности на основе унифицированных стандартов должен быть одним из необходимых элементов набора документов для допуска ВАТС к эксплуатации.

Обязательным требованием является своевременное и быстрое уведомление водителей о наличии проблем с кибербезопасностью; поскольку устранение угрозы или последствий взлома зай-

мёт некоторое время, водитель или АСВ должны предпринимать корректирующие действия.

Следует контролировать жизненный цикл ПО — своевременно обновлять ПО как транспортного средства, так и взаимодействующих с ним объектов дорожно-транспортной инфраструктуры, причём вновь установленное ПО должно обладать всеми необходимыми сертификатами безопасности.

Дополнительные требования могут также включать в себя схему отчётности, в которой сообщается о возможных неисправностях ТС и потенциальных уязвимостях для кибератак, требования по борьбе с кибератаками, включая решения по их обнаружению, предотвращению и мониторингу угроз.

Следует принимать корпоративные правила кибербезопасности и охраны данных в организациях, которые имеют отношение к производству и обслуживанию подключённых и высокоавтоматизированных транспортных средств. Необходимо предоставлять соответствующие полномочия сотрудникам службы безопасности вышеуказанных организаций, чтобы предотвратить уязвимости или ошибки, прежде чем транспортное средство получит допуск к коммерческой эксплуатации.

Не следует рассматривать кибербезопасность подключённых и автоматизированных ТС по отдельным компонентам и проблемам, необходим многоуровневый подход и обеспечение системных мер защиты. Целостный подход достигается путём рассмотрения проблемы как комплекса вопросов и системных решений. ■

Литература:

1. Комплекс стандартов ГОСТ Р ИСО 26262. Дорожные транспортные средства. Функциональная безопасность.
2. Проект «Концепция обеспечения безопасности дорожного движения с участием беспилотных транспортных средств на автомобильных дорогах общего пользования».
3. Технологические барьеры НТИ // Национальная технологическая инициатива. URL: <https://nti2035.ru/technology/barriers.php> (дата обращения: 27.11.2019)
4. Шарапов И. Военные против 5G: что потеряет Россия без нового стандарта связи // Официальный сайт Forbes. URL: <https://www.forbes.ru/tehnologii/374291-voennye-protiv-5g-chto-poteryaet-rossiya-bez-novogo-standarta-svyazi> (дата обращения: 27.11.2019)
5. Кашин С. Как на транспорте большие данные превратились в ценный актив // Официальный сайт газеты «Гудок». URL: https://www.gudok.ru/science_education/?ID=1463049 (дата обращения: 27.11.2019)