DOI: 10.18721/JE.13501
УДК 338.47 : 330.47 : 656.13 : 004.056

РАЗВИТИЕ ИНТЕЛЛЕКТУАЛЬНЫХ ТРАНСПОРТНЫХ СИСТЕМ В РОССИЙСКОЙ ФЕДЕРАЦИИ: ОПРЕДЕЛЕНИЕ ТРЕБОВАНИЙ И ОРГАНИЗАЦИЯ СОЗДАНИЯ ПОЛИГОНОВ ТЕСТИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Писарева О.М.[1], Алексеев В.А.[2], Медников Д.Н.[1], Стариковский А.В.[1]

[1] ФГБОУ ВО «Государственный университет управления», Москва, Российская Федерация;

[2] ООО «Рабус», Москва, Российская Федерация

Технологии беспилотного транспорта создают новые возможности развития экономической и социальной инфраструктуры стран и регионов. Реализация проектов умной мобильности наряду с качественными преобразованиями сфер транспортных и логистических услуг связана с необходимостью идентификации и оценки рисков широкого внедрения беспилотных автомобилей. Масштаб и интенсивность цифровых коммуникаций при эксплуатации высокоавтоматизированных транспортных средств различного назначения расширяет сферу обеспечения безопасности дорожного движения. Беспроводная связь является основным каналом информационного взаимодействия динамических и статических объектов интеллектуальной транспортной системы, что предопределяет формирование специфического набора угроз. Повышение уровня рисков электромагнитных возмущений и преднамеренных воздействий на управление беспилотными автомобилями выводит на первый план анализ вопросов информационной безопасности. Это требует разработки новых нормативных и технических подходов к обеспечению безопасности дорожного движения. В статье представлен анализ текущего состояния проектов создания национальных интеллектуальных транспортных систем. Определены ключевые характеристики источников угроз и зон уязвимости технологической платформы информационного взаимодействия высокоавтоматизированных транспортных средств. Приведены ключевые требования к определению состава и разработке спецификации задач испытательных полигонов при тестировании информационной безопасности беспилотных автомобилей. Обобщен опыт проектирования испытательных полигонов и предложен авторский вариант процесса организации разработки и реализации подобного проекта, учитывающего весь спектр задач верификации и валидации компонентов интеллектуальной транспортной системы с позиции обеспечения безопасности информационного взаимодействия с учетом возможностей технологической платформы V2X в среде мобильной связи 5G. Представлены авторские рекомендации по созданию в Российской Федерации институциональных условий для регулирования создания и сертификации устройств и технологий информационного взаимодействия беспилотных автомобилей. Определены приоритетные направления дальнейших исследований в области разработки аппаратно-программных решений и технологических регламентов (стандартов) для обеспечения информационной безопасности, а также формирования методики и инструментария тестирования беспилотных автомобилей различного назначения в Российской Федерации.

Ключевые слова: интеллектуальная транспортная система, цифровые технологии, беспилотный транспорт, информационная безопасность, испытательный полигон, организация тестирования

Ссылка при цитировании: Писарева О.М., Алексеев В.А., Медников Д.Н., Стариковский А.В. Развитие интеллектуальных транспортных систем в Российской Федерации: определение требований и организация создания полигонов тестирования информационной безопасности // Научно-технические ведомости СПбГПУ. Экономические науки. 2020. Т. 13, № 5. С. 7–23. DOI: 10.18721/JE.13501

DEVELOPMENT OF INTELLIGENT TRANSPORT SYSTEMS IN THE RUSSIAN FEDERATION: DEFINING REQUIREMENTS AND ORGANIZING THE CREATION OF INFORMATION SECURITY TESTING GROUNDS

O.M. Pisareva[1], V.A. Alexeev[2], D.N. Mednikov[1], A.V. Starikovsky[1]

[1] State University of Management,
Moscow, Russian Federation;
[2] Rabus LLC,
Moscow, Russian Federation

Autonomous vehicle technologies create new opportunities for the development of the economic and social infrastructure of countries and regions. Implementation of smart mobility projects, along with qualitative transformations in the areas of transport and logistics services, is associated with the need to identify and assess the risks of the widespread introduction of autonomous vehicles. The scale and intensity of digital communications in the operation of highly automated vehicles for various purposes expands the scope of road safety. Wireless communication is the main channel of information interaction between dynamic and static objects of an intelligent transport system, which predetermines formation of a specific set of threats. The increase in the risk of electromagnetic disturbances and deliberate impacts on the management of autonomous vehicles brings the analysis of information security issues to the fore. This requires an urgent start to develop new regulatory and technical approaches to road safety. The article presents an analysis of the current state of projects for the creation of national intelligent transport systems. The key characteristics of sources of threats and zones of vulnerability of the technological platform for information interaction of highly automated vehicles have been determined. The key requirements to determine the composition and develop the specification of the tasks of the testing grounds when testing the information security of autonomous vehicles are given. The authors generalized the experience of designing test sites and proposed their version of the process of organizing the development and implementation of such a project. The authors considered the whole range of tasks of verification and validation of the components of an intelligent transport system from the standpoint of ensuring the security of information interaction, taking into account the capabilities of the V2X technology platform in a 5G mobile communications environment. The authors presented recommendations on introducing institutional conditions to regulate the creation and certification of devices and technologies for information interaction of autonomous vehicles in the Russian Federation. The priority of the further research is placed on developing hardware and software solutions and technological regulations (standards) for information security, as well as on forming methods and tools for testing self-driving cars for various purposes in the Russian Federation.

Keywords: intelligent transport system, digital technologies, autonomous vehicles, information security, testing ground, testing organization

Citation: O.M. Pisareva, V.A. Alexeev, D.N. Mednikov, A.V. Starikovsky, Development of intelligent transport systems in the Russian Federation: defining requirements and organizing the creation of information security testing grounds, St. Petersburg State Polytechnical University Journal. Economics, 13 (5) (2020) 7–23. DOI: 10.18721/JE.13501

Введение

Создание отечественной интеллектуальной транспортной системы и развитие беспилотного автомобильного транспорта (общественного, коммерческого и государственного) с учетом пространственной специфики нашей страны является важнейшим направлением развития цифровой экономики в Российской Федерации.

В рамках работы Наблюдательного совета Агентства стратегических инициатив 18 сентября 2019 г. Президент Российской Федерации В.В. Путин отметил, что появились новые технологии, которые поменяют и уже изменяют мир[1]. В частности, в составе технологий, определяю-

[1] РИА Новости. 17.05.2020. URL: https://ria.ru/20200517/1571580444.html

щих сохранение и развитие русской цивилизации, президент выделил искусственный интеллект и беспилотную технику. Оба этих направления технологически переплетаются при создании интеллектуальной транспортной системы (ИТС). Построение ИТС, представляющей интегрированный комплекс взаимодействующих подсистем и элементов, является, независимо от ее масштаба, сложнейшей технической и организационной задачей. Следуя принципу интероперабельности, для обеспечения бесшовного *трансграничного* движения беспилотных транспортных средств, создаваемые ИТС различного уровня (в том числе в рамках ЕАЭС) должны функционировать по единому регламенту и использовать одинаковые технологии.

Беспроводные каналы связи и цифровые устройства управления высокоавтоматизированных транспортных средств (ВАТС) различного назначения формируют новый набор угроз, проявляющихся при взаимодействии подключенных и автономных автомобилей между собой и другими транспортными средствами, а также с дорожной инфраструктурой (ДИ), центрами управления автомобильным движением (со стороны регулятора) и центрами управления эксплуатацией ВАТС (со стороны владельца/оператора). Использование в рамках технологии беспилотных автомобилей беспроводных коммуникаций, распределенных центров хранения и обработки больших данных, бортовых компьютеров, контроллеров и иных электронных устройств связано с возрастающей опасностью деструктирующего случайного и умышленного электромагнитного воздействия на штатный режим функционирования региональных, национальных и международных интеллектуальных транспортных систем (ИТС).

Бесспорно, что при масштабном распространении беспилотного автомобильного движения в России проблематика обеспечения информационной безопасности ИТС как технологической платформы взаимодействия ВАТС с ДИ приобретает существенное значение для мониторинга дорожной обстановки, регулирования дорожного трафика и снижения аварийности. Объект настоящего исследования — транспортная система Российской Федерации в условиях расширения спектра используемых цифровых технологий в создании систем управления транспортного средства и комплексов организации и регулирования движения. Предметом исследования является безопасность функционирования беспилотных автомобилей в умной среде дорожного сообщения. Это требует рассмотрения вопросов и решения задач обеспечения информационной безопасности взаимодействия подключенных и автономных автомобилей между собой, а также с другими транспортными средствами, дорожной инфраструктурой и центрами управления беспилотными перевозками пассажиров и грузов. В этой связи необходимо в том числе пристальное изучение и анализ любого положительного опыта в области организации проектирования и создания полигонов тестирования систем кибербезопасности беспилотных автомобилей, что позволит усовершенствовать организационное и методическое обеспечение обоснования государственных программ и коммерческих проектов развития беспилотных технологий и интеллектуальной транспортной системы в нашей стране.

Предпосылки и цель исследования

Прогресс в области информационно-коммуникационных технологий стремительно преобразует социально-экономический ландшафт современных государств. Возросший в начале 2020-го г. спрос на оказание бесконтактных услуг и повсеместный переход к режиму удаленной работы показал перспективные ниши развития ICT-решений для различных секторов национальной экономики и сфер публичной власти. Однако на этом фоне специалисты выявляют существенные просчеты в работе цифровых технологий, связанных с развитием инфраструктуры систем передачи данных и обеспечением информационной безопасности, которые пока не рассчитаны на пиковые нагрузки и масштабную защиту юридически значимых транзакций. Кроме того, с развитием интернета вещей к действующим абонентам прибавятся умные машины и механизмы, которые резко увеличат нагрузку на сети связи общего и специального назначения.

Примерно с 2015 г. явно наметилась тенденция резкого увеличения количества подключенных устройств. По оценкам экспертов, к 2025 г. в мире ожидается расширение рынка интернета вещей до 40 млрд единиц[2]. Распространение беспилотных технологий также предъявляет дополнительные требования к качеству информационно-коммуникационных решений для обработки и защиты больших объемов персонализированных данных владельцев, операторов и пользователей подключенных и автоматизированных транспортных средств (Connected and Automated Vehicles, CAV[3]) в среде ИТС. Хотя прогнозируемая доля ВАТС относительно не велика (не более 3–4%%), необходимо учитывать, что к сегменту IoT в рамках ИТС относится строительная и дорожная техника, элементы регулирования движения (светофоры, дорожные знаки, информационные табло и др.). Дополнительную нагрузку на сети связи создают смартфоны, планшеты и другие мобильные устройства, которыми пользуются пешеходы, водители и пассажиры. Все это формирует устойчивый и возрастающий спрос на качественную сетевую инфраструктуру дороги, которая должна обеспечить потребность в различных сервисах без ущерба каналу взаимодействия ВАТС с ДИ.

Эффективная и надежная эксплуатация беспилотных транспортных средств в общественных и личных, государственных и коммерческих целях зависит от обеспечения необходимого уровня безопасности беспилотных транспортных и логистических услуг. Учитывая аппаратно-программную основу построения ИТС и большой объем накапливаемой и обрабатываемой в ней конфиденциальной информации и персональных данных, поддержание надежности и снижение рисков функционирования беспилотного транспорта связано, прежде всего, с решением задач информационной безопасности[4].

По широкому кругу вопросов, связанных с безопасностью физических и киберфизических систем, ключевым моментом является обеспечение информационной безопасности взаимодействия беспилотного транспортного средства с дорожной инфраструктурой и другими участниками движения на автомобильных дорогах различного назначения. Главная цель проводимого исследования состоит в определении эффективных организационно-технических решений при создании и развитии испытательных полигонов для тестирования безопасности эксплуатации технологических платформ информационной интеграции управления беспилотным автомобилем и дорожной инфраструктурой. В этой связи для успешной организации работ по внедрению элементов ИТС в реальную хозяйственную практику важно оценить:

– существующие подходы к обеспечению безопасности информационного взаимодействия CAV с элементами ITS (так называемая технологическая платформа — Vehicle-to-Everything или V2X);

– текущее состояние разработок в области проектирования и создания испытательных полигонов для комплексного тестирования методов и средств обеспечения безопасности беспилотного транспорта в различных режимах/условиях его эксплуатации.

Такую работу необходимо проводить скоординировано, с участием как проектировщиков, производителей и пользователей беспилотных транспортных средств и интеллектуальных элементов дорожной инфраструктуры, так и регулирующих и контрольных органов. Важно разви-

[2] См., например, отчет международной консалтинговой копании Strategy Analytics Research Services. URL: https://www.strategyanalytics.com/access-services/devices/connected-home/consumer-electronics/reports/report-detail/global-connected-and-iot-device-forecast-update.

[3] Отметим, что на международном уровне в специализированных исследованиях онтологическая модель для описания интеллектуальной транспортной системы (Intelligent Transportation Systems, ITS) еще не устоялась. Для обозначения автоматизированных автомобилей в специализированной литературе используются альтернативные термины, определяющие идентичную с CAV сущность, как правило, без привязки к степени автоматизации функций вождения. Например, Департаментом транспорта США в официальной программе развития интеллектуального транспорта введено понятие Connected Vehicles, CV (Intelligent Transportation System Strategic Plan 2015-2019 / The United States Department of Transportation. Washington, DC: US DOT, 2014. URL: https://www.its.dot.gov/index.htm). Для характеристики беспилотных наземных транспортных средств в США также применяют понятие Unmanned Ground Vehicles, UGV [1]; в Китае — Intelligent and connected vehicles, ICV (см. обзор [2]), в России часто употребляется термин «высокоавтоматизированное транспортное средство» (см., например, [3]), а в Сингапуре при подготовке официальных документов и в публикациях специалистов по организации автоматизированного движения — Autonomous vehicles, AV (см., например, [4]).

[4] Cybersecurity guidebook for cyber-physical vehicle systems (SAE J3061-2016) / SAE International. Troy, Michigan: SAE International, 2016. URL: http://standards.sae.org/j3061_201601/

вать требования к стандартизации обеспечения информационной безопасности CAV. Знание аппаратно-программных и информационно-коммуникационных уязвимостей CAV позволит разработчикам точно идентифицировать проблемные зоны и диагностировать критические риски при реализации задач развития беспилотного транспорта в Российской Федерации.

Результат указанных действий позволит определять необходимые меры по изменению правовых основ и организационного механизма эксплуатации ВАТС и функционирования ИТС, а также стандартизации технической базы и унификации аналитического инструментария проверки и оценки уровня информационной безопасности систем автоматизированного/автономного управления беспилотных автомобилей. Это обеспечит создание условий для рациональной и эффективной реализации требований Указа Президента Российской Федерации от 07 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 г.» в части инновационного развития перспективных технологий и обеспечения высокой конкурентоспособности отечественной экономики на глобальном рынке продукции и услуг с высокой добавленной стоимостью.

Обзор литературы и исследований

Исследования и разработки в сфере создания технологий для наземного, воздушного и водного беспилотного транспорта ведутся в мире достаточно давно [5, 6]. Имеются свои оригинальные технические решения и у российских ученых, конструкторов и инженеров [7, 8]. В настоящее время спектр и уровень имеющегося научно-технического задела по беспилотным технологиям перевел проблему их эксплуатации в сферы нормативного и организационного обеспечения проектов внедрения и распространения беспилотных автомобилей различного функционального назначения. Россия активно включилась в работу по формированию институциональных основ и технических средств для создания собственной интеллектуальной транспортной системы. Так, в 2011 г. при Госстандарте России был создан технический комитет ТК 57 «Интеллектуальные транспортные системы», на который приказом Госстандарта России от 22 июля 2011 г. № 3821 были возложены полномочия по организации работ в области стандартизации разработки и эксплуатации беспилотного транспорта. Технические, информационные, технологические аспекты проектирования и разработки беспилотного транспорта охарактеризованы в работах [9–13]. Правовые, организационные, экономические аспекты построения инфраструктуры автомобильных дорог общего и специального назначения для эксплуатации CAV рассмотрены в работах [14–17][5]. Задачи и методы обеспечения информационной безопасности CAV и ИТС представлены в работах [18–21][6].

Дополнительной эмпирической базой исследования стал широкий спектр разнообразных источников: нормативные правовые и стратегические плановые документы, статистические данные, научные и специализированные публикации, информационно-справочные и методические материалы международных организаций, включая данные интернет-сайтов ООН (http://www.un.org), ЕАЭС[7] (http://www.eaeunion.org/), ОЭСР (http://www.oecd.org) и др., отчеты о проведении национальных и международных научно-практических и экспертных мероприятий.

При изучении состояния и результатов проведения научно-практических работ в рассматриваемой предметной области авторами применялись методы контентного и семантического, логического и статистического, сравнительного и экспертного анализа. Вместе с тем, задачи обобщения положений национальных стратегических планов развертывания ИТС и нормативных требова-

[5] См. также: The economic and social value of autonomous vehicles. Compass Transportation and Technology, Inc. 2018. 58 p.

[6] См. также: Safety first for automated driving. 2019. 157 p. URL: https://www.aptiv.com/docs/default-source/white-papers/safety-first-for-automated-driving-aptiv-white-paper.pdf

[7] В рамках ЕАЭС ключевые вопросы интеграции и координации деятельности стран-участниц в области ИТС решаются в рамках реализации цифровой повестки Евразийского экономического союза до 2025 г. (https://digital.eaeunion.org/extranet/) и профильных подразделений Евразийской экономической комиссии (Департамент транспорта и инфраструктуры, Департамент технического регулирования и аккредитации).

ний к обеспечению безопасности беспилотного транспорта, унификации разработки методического и аналитического инструментария для анализа и оценки информационной безопасности технологической платформы взаимодействия CAV с дорожной инфраструктурой, а также задачи формирования подходов к проектированию испытательных полигонов для тестирования устойчивости систем управления беспилотного транспорта к различным видам и способам нарушения корректности его коммуникаций с экосистемой V2X ждут своих решений.

Методология и результаты исследования

С системных позиций развитие технологий автоматизации автомобильного движения следует рассматривать как следствие общего процесса цифровой трансформации в информационном обществе. Современные компьютерная техника и коммуникационное оборудование создают предпосылки для радикальной реструктуризации национальной экономики. Инновационные проекты индустриального и инфраструктурного назначения в цифровой экономике отличает *комплексность* используемых базовых (сквозных) технологий нового поколения. В частности, для создания беспилотных транспортных средств и построения интеллектуальной транспортной системы активно используются методы и технологии беспроводной связи, больших данных, искусственного интеллекта, распределенных реестров, робототехники и сенсорики. В свою очередь, новые возможности беспилотных автомобилей оказывают широкое воздействие на бизнес-процессы и меняют облик обслуживаемых отраслей, адаптируя сопряженные технические и организационные решения для взаимодействующих экономических и социальных агентов в экосистеме интеллектуального транспорта.

С одной стороны, масштабная автоматизация через развитие кооперативных транспортных систем и интеллектуальной мобильности направлена на снижение рисков в процессе транспортировки, с другой стороны, цифровизация автомобилей и дорожной инфраструктуры через появление *новых* зон уязвимости и направлений угроз для совокупности взаимодействующих между собой киберфизических систем приводит к повышению рисков автономного (автоматизированного) движения транспортных средств. Поэтому разработка технологий CAV нуждается в оценке последствий использования, что требует комплексного рассмотрения структуры взаимосвязей в киберфизических системах интеллектуального автомобильного транспорта.

Появление протокола связи между отдельными машинами (Vehicle-to-Vehicle, V2V — подсистема интернета вещей) и их использование в автомобильных системах открыло путь для новых технологий: системы связи между автомобилем и пешеходом (Vehicle-to-Pedestrian, V2P), между автомобилем и отдельным устройством (Vehicle-to-Device, V2D), между электромобилем и электросетью (Vehicle-to-Grid, V2G), между автомобилем и элементами умных домов (Vehicle-to-Home, V2H), между автомобилем и сетью связи (Vehicle-to-Network, V2N), между автомобилем и элементами дорожной инфраструктурой (Vehicle-to-Infrastructure, V2I), т.е. в широком смысле сетевых технологий на транспорте.

Освоение следующего поколения мобильной связи 5G создает предпосылки и базу для построения механизма эффективных взаимодействий в рамках ИТС по различным плоскостям (slice): умный транспорт подразумевает использование коммуникаций по принципу V2X (Vehicle-to-Everything), где поддерживается среда обмена данными между автомобилями и различными элементами окружения дорожной сети общего и выделенного пользования.

С переходом к протоколам и устройствам мобильной связи 5G появилась возможность построения единой технологической платформы высокоскоростного обмена электронными данными и применения методов искусственного интеллекта в общей цифровой среде между автомобилем и различными элементами (субъектами и объектами) внешнего окружения в целостной интеллектуальной транспортной системе с поддержанием динамических коммуникаций для комплекса аппаратно-программных решений V2X. При этом, в отличие от ряда других стран, Россия при-

держивается технологической нейтральности в вопросе выбора стандарта для V2X и тестирует на полигоне ФГУП «НАМИ»[8] разные варианты построения технологической платформы связи в рамках ИТС.

В этих условиях необходима активизация согласованной и комплексной работы в области технического нормирования, регулирования, стандартизации и поддержки инновационных проектов разработки информационно-технологических решений для российских прототипов CAV [8, 22 и др.]. Синтез лучших идей, практик и технологий позволяет минимизировать издержки и недостатки экспериментального периода разработки элементов и инфраструктуры ИТС.

Стратегиями и дорожными картами развития национальных ИТС в странах, лидирующих по беспилотным технологиям[9], предусматривается первостепенное решение задач поэтапного обеспечения безопасности для различной категории транспортных средств. В соответствии с устоявшейся практикой и принятыми стандартами технологии подразделяются на 5 уровней автоматизации автомобилей: от «1» (функция помощи водителю) до «5» (полная автоматизация вождения); уровень «0» обозначает отсутствие автоматизированных компонентов в системе управления транспортным средством. Для Российской Федерации, не охваченной указанным обзорным исследованием KPMG в области развития технологий беспилотных автомобилей, в условиях существования значительного научно-технического задела и подготовленных инженерных кадров в области автоматического управления сложными техническими системами следование тактике догоняющего развития при создании и внедрении CAV может принести определенные преимущества: синтез лучших идей, практик и технологий позволит минимизировать издержки и недостатки экспериментального периода разработки элементов и инфраструктуры ИТС.

На наш взгляд, наиболее представительными и полезными для анализа являются официальные нормативные материалы планирования развития беспилотного транспорта в странах Европейского Союза, США, Китае, Японии, Южной Кореи и Сингапуре. В табл. 1 представлена обобщенная информация о национальных инициативах в области беспилотного автомобильного движения и его безопасности.

Обзор возможных подходов к анализу проблем надежности эксплуатации CAV и построению концептуальных основ обеспечения информационной безопасности в среде ITS представлен в работе [23]. Приведенные в ней положения основаны на результатах разработки общего видения по взаимодействию при развертывании интеллектуальных транспортных систем (Cooperative Intelligent Transport Systems, C-ITS), разработанного в интересах Европейской комиссии[10]. Это нашло свое дальнейшее развитие в Европейской стратегии по кооперативным интеллектуальным транспортным системам C-ITS, принятой 30 ноября 2016 г.

Рекомендации предполагают структуризацию задачи обеспечения информационной безопасности технологической платформы V2X в рамках описания стратегической модели киберфизических систем и инфраструктуры транспортных средств. Механизм взаимодействия автономного транспортного средства с физической и киберфизической инфраструктурой формируется комплексным использованием технологий интеллектуальной мобильности: автоматизации; цифрового интерфейса; информационной взаимосвязанности и цифровых данных. Оценка надежности технологической платформы V2X связана с исследованиями возможностей и последствий влияния на указанные функциональные зоны автоматизации угроз, исходящих из различных источников и с различными целями.

[8] Проведены испытания технологий ITS-G5 стандарта ETSI и C-v2x стандарта 3GPP // Вестник ГЛОНАСС. 30.03.2019. URL: http://vestnik-glonass.ru/news/tech/standarty-obespecheniya-svyazi-podklyuchennykh-avtomobiley-otrabotayut-v-nami/

[9] Наиболее авторитетным средством мониторинга готовности стран к созданию ITS является разрабатываемый консалтинговой компанией KPMG «Индекс готовности автономных транспортных средств»: последний отчет был подготовлен в 2019 г. URL: https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf.

[10] Исследовательский проект, инициированный в ноябре 2014 г., позволил принять 30.11.2016 г. Европейскую стратегию по кооперативным интеллектуальным транспортным системам C-ITS. URL: https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf; https://ec.europa.eu/transport/sites/transport/files/2017-09-c-its-platform-final-report.pdf

Таблица 1. Базовые национальные инициативы в области беспилотного автомобильного движения и обеспечения его безопасности
Table 1. General basic national initiatives on self-driving and safety

Страны	Базовый документ	Аспект/область лучшей практики
Европейский Союз	Стратегия по подключенной и автоматизированной мобильности[11]	структурированность и согласованность стратегических инициатив развития ITS
США	Стратегический план интеллектуальных транспортных систем на период 2015–2019[12]	масштабность намеченных преобразований и пионерские решения Society of Automotive Engineers, SAE, и The National Highway Traffic Safety Administration, NHTSA, для стандартизации беспилотного автотранспорта, включая область безопасности
КНР	Дорожная карта по развитию технологий интеллектуальных транспортных средств[13]	близость исходных условий развития и относительная политическая доступность тиражируемых технологий беспилотного транспорта
Япония	Межведомственная программа содействия стратегическим инновациям: автоматическое вождение для универсальных услуг[14]	уровень инженерно-технических и организационно-технологических решений для автоматизации автомобильного движения в урбанизированном пространстве
Южная Корея	Генеральный план развития автомобильной индустрии[15]	темпы изменений и степень централизации государственных решений по мобилизации и координации участников рынка беспилотных технологий и систем на основе Национальной стратегии 4-й промышленной революции
Сингапур	Инициатива для автономных автомобилей[16]	комплексность, компактность и завершенность согласованных решений для приближения к «идеальному» общественному образу ITS в рамках проекта «Умной мобильности»

Источник: Подготовлено авторами

В ряде исследовательских работ проводится анализ уязвимости моделей транспортных систем с различным уровнем автоматизации [24 и др.], для которых определяется типология дистанционных атак в зависимости от трех категорий характеристик беспилотных автомобилей: зона для удаленной атаки, киберфизические особенности транспортного средства, используемая сетевая архитектура.

В частности, в работе [25] выделено семь основных категорий дистанционных атак, основанных на анализе характеристик 20 моделей транспортных средств. Это исследование установило очевидную тенденцию роста возможных потенциальных векторов атаки для новейших автомобилей с технологиями автоматизированного управления вождением (Connected Automated Driving, CAD), что подчеркивает важность проведения дополнительных исследований в области обеспечения безопасности платформы V2X для разработки более эффективных способов и средств защиты от угроз умышленного негативного воздействия в цифровой среде ИТС (с желательным опережением характеристик перспективных/прогнозируемых методов взлома контура безопасности киберфизической системы CAV).

Возможный подход к построению комплексной модели угроз для автоматизированных систем вождения, включая внешние атаки, в рамках платформы V2X и разработке метода оценки атак через различные каналы телекоммуникации предложен К. Окуямой[17]. Он обобщил первые

[11] The European Union strategy on connected and automated mobility. URL: https://ec.europa.eu/transport/
[12] Intelligent Transportation System Strategic Plan 2015-2019. URL: https://www.its.dot.gov/
[13] The SAE China's technology roadmap for energy-saving and new energy vehicles. URL: http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757018/c5600356/content.html
[14] The Cross-ministerial Strategic Innovation Promotion Program (SIP): Automated Driving for Universal Services (ADUS). URL: https://en.sip-adus.go.jp/sip/
[15] The national master plan of the automotive industry development. URL: https://www.molit.go.kr/english/USR/WPGE0201/m_36859/DTL.jsp
[16] The Singapore autonomous vehicle initiative. URL: https://www.lta.gov.sg/savi-step-towards-autonomous-transport.html
[17] Okuyama K. Formulation of a comprehensive threat model for automated driving systems including external vehicular attacks such as V2X and the establishment of an attack evaluation method through telecommunication. SIP-adus: Project Reports, 2014-2018. Automated Driving for Universal Services. Cabinet Office, Government of Japan, 2019, pp. 77–83.

результаты реализации в Японии проекта ADUS программы SIP на основе комбинации методов кластеризации, статистического анализа и нечетких множеств (для структурирования и идентификации уровня угроз в номинальной шкале).

Анализ общей практики разработки и испытаний CAV показывает, что в целом эксперты [26, 27][18] связывают основные перспективы построения и функционирования национальных интеллектуальных транспортных систем и международных транспортных коридоров с платформами V2X в рамках развития инфраструктуры сотовых сетей нового поколения. При этом для создания эффективной ИТС потребуется использование комплекса технологий связи. Например, специалистами немецкого исследовательского центра Huawei была дана характеристика использования спектра будущих технологий — разрабатываемых в интересах мобильной связи высокочастотных (свыше 6 ГГц) и широкополосных диапазонов (mmWav для 60 Гц), а также оптических каналов связи (VVLC для 485-789 ТГц), которые будут включены в архитектуру сети доступа для платформы V2X (см. табл. 2).

Таблица 2. Требования к коммуникационной инфраструктуре ИТС для различных режимов использования платформы V2X (специфика проектирования архитектуры сети)
Table 2. Requirements for communication infrastructure of ITS for various modes of use of the V2X platform (specifics of network architecture design)

Тип использования	Режим V2X	Сквозная задержка (ms)	Надежность	(Kbps)	Спектр связи
Совместная осведомленность	V2V/V2I	100-1000	90-95%	5-96	короткий и средний
Совместное восприятие	V2V/V2I	3-1000	95%	5-25000	короткий
Совестное маневрирование	V2V/V2I	3-1000	99%	10-5000	короткий и средний
Обзор уязвимых участников	V2P	100-1000	95%	5-10	короткий
Управление эффективностью движения	V2N/V2I	1000	90%	10-2000	длинный
Вождение с телеоператором	V2N	5-20	99%	25000	длинный

Источник: https://www.huawei.eu/what-we-do/car-connectivity

Проведение тестирования информационной безопасности беспилотных транспортных средств при воспроизведении реальных условий эксплуатации (до периода испытаний на выделенных участках дорожной сети и/или на дорогах общего пользования, если это разрешается национальными стандартами), как правило, осуществляется в два этапа: 1) проводятся эксперименты с отработкой угроз случайного и умышленного нарушения контура информационной защиты CAV в специализированных лабораториях, в том числе с тестовыми площадками ограниченного размера, 2) выполняются проверки надежности на полигонах с воспроизведением различных участков дорожной сети и окружающего городского и природного ландшафта. Испытательные полигоны в автомобильной промышленности используются давно и широко, решая задачи тестирования образцов новых/модернизированных транспортных средств и оценки различных их характеристик: уровень выбросов, динамика автомобиля, надежность механизмов и системы управления, прочность конструкции, защищенность водителя и пассажиров и т.д. Од-

[18] См. также: PEGASUS method: An overview. 2019. 33 p.; Automated vehicles index: 1Q, 2016. Munich, Roland Berger GmbH, 2015. 18 p.; Berger C. Automating acceptance tests for sensor- and actuator-based systems on the example of autonomous vehicles. Aachen, Shaker Verlag, 2010. 272 p.

нако, как правило, традиционные испытательные полигоны не имеют возможности тестировать все различные характеристики вождения CAV [26], а также оценивать различные сценарии автоматизированного вождения, имеющие отношение к оценке функциональных режимов и информационной безопасности CAV в среде сетевых коммуникации. Таким образом, дополнительно к общим проверкам систем и устройств пассивной и активной безопасности общей конструкции автомобиля необходимо тестирование безопасности информационного взаимодействия исправного CAV, которое может осуществляться в виртуальной (математическое и компьютерное моделирование работы программного и аппаратного обеспечения автомобиля и его компонентов) и реальной (лабораторные и полигонные испытания полностью или частично укомплектованного автомобиля и его компонентов) среде для различных сценариев реализации факторов риска нарушения системы управления автомобиля.

Анализ научных публикаций и доступных информационных материалов показал, что в настоящее время отсутствует какой-либо единообразный концептуальный подход к разработке проекта испытательного полигона для CAV. Тем не менее, можно найти определенные методические рекомендации [26] по использованию *субъективных критериев* для оценки эффективности испытательного полигона (на стадиях его проектирования и создания) на основе целевой коллективной дискуссии (экспертизы) с участием представителей научных кругов, бизнеса и государственных чиновников при обсуждении проекта его создания. В частности, исследователи из Мичиганского университета[19] предлагают исходить при разработке концепции, планировки и спецификации испытательного полигона из *обобщенных характеристик* множества ключевых дорожных ситуаций при различных сценариях эксплуатации беспилотных автомобилей в разнообразных погодных условиях и моделях поведения водителей обычных транспортных средств. Попытка применить *количественные метрики* для оценки различных характеристик испытательного полигона и проверки структуры его наземных дорог представлена в работах [28, 29 и др.]. Как правило, предлагается использовать непараметрический байесовский метод обучения на основе экспериментальных наборов данных с выборочной оптимизацией для оценки совместимости характеристик между различными базовыми сценариями дорожного движения. Большинство авторов предлагают общий подход на основе описания типичных случаев эксплуатации CAV и реальных событий вождения в естественных условиях. Это гипотетически позволяет использовать методы оптимизации при проектировании полигона с использованием ограниченного количества дорожных активов (элементов дорожной инфраструктуры) для выработки обоснованного суждения о показателях качества тестируемых экземпляров интеллектуальных транспортных средств различного назначения и уровня автоматизации.

В целом при различии предложений о методологии проектирования испытательных полигонов для CAV можно выделить одно общее положение — исходной точкой разработки проекта является определение основной цели процесса тестирования, которая должна быть декомпозирована/классифицирована по следующим ключевым аспектам проверки компонент и системы автоматизированного вождения:

– работоспособность и совместимость;
– надежность функционирования;
– долговечность эксплуатации;
– информационная безопасность (кибербезопасность);
– целостность данных и защита конфиденциальности.

В свою очередь, параметры полигона и условия испытаний CAV должны:

– учитывать различные проблемы при тестировании технологий в зависимости от вариантов использования, функций и выбранных уровней автоматизации движения;

[19] Peng H., McGuire G. Mcity ABC test: A concept to assess the safety performance of highly automated vehicles. University of Michigan, 2019. 15 p.

– воспроизводить детерминированные или стохастические ситуации тестирования в реальной или виртуальной среде;

– предоставлять возможность проверять функции автоматического вождения воспроизводимым и эффективным способом при решении задач государственной сертификации CAV;

– позволять проводить оценку ответственности и страховать риски владельца/оператора CAV.

Исходя из сформулированной цели создания тестовой площадки, организация проектирования испытательного полигона должна включать этап предварительного согласования заинтересованными сторонами его спецификации для уточнения набора стандартных и специальных задач проверки характеристик технологий и систем CAV. Т.е. планировка и оборудование и полигона должна учитывать все необходимые требования для проверки функций автоматизированного вождения с выбранных/заданных позиций (например, обеспечение кибербезопасности). Набор необходимых элементов испытательного полигона, а также соответствующее оборудование исследовательских лабораторий и контрольного исследовательского центра определяются локализацией задач в рассмотренной ранее пирамиде испытаний и проверок в рамках так называемой V-модели тестирования CAV [30 и др.]).

В общем случае, обобщая положения работ [27, 31, 32 и др.], можно отметить, что спецификация полигона для оценки информационной безопасности платформы V2X должна включать возможность тестирования следующих компонент:

– общая архитектура автономного транспортного средства;

– оборудование системы автоматизированного вождения;

– программное обеспечение системы автоматизированного вождения.

При этом тестирование должно проводиться в условиях симуляции угроз как в лаборатории (Simulation Testing), так и в движении (Driving Testing).

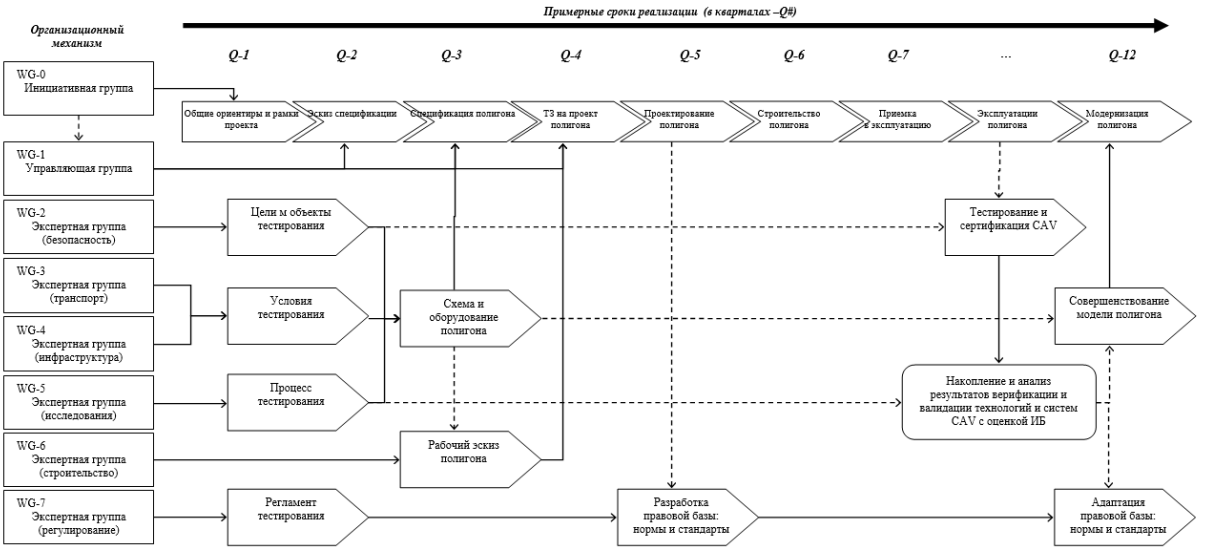

Рис. 1. Схема процесса разработки и реализации проекта испытательного полигона тестирования безопасности информационного взаимодействия технологической платформы V2X

Fig. 1. Integrated diagram of the development and implementation process of the project for testing the security of information interaction of the V2X technological platform

Источник: подготовлено авторами на основе [26, 31] и Cybersecurity guidebook for cyber-physical vehicle systems (SAE J3061-2016) (использованы обозначения: ИБ — информационная безопасность; WG — рабочая группа).

Кроме того, спецификация полигона должна обеспечивать тестирование уязвимостей CAV для оценки следующих функций: 1) восприятие; 2) принятие решений; 3) навигация; 4) управление действиями [33 и др.].

При проектировании испытательного полигона в рамках формирования общего подхода к валидации системы автоматизированного вождения транспортного средства необходимо разработать схему процесса оценки. Независимо от использования конкретных методов проведения испытаний, процесс оценки характеристик обеспечения информационной безопасности CAV должен включать следующие этапы:

– определение наборов функционального тестирования;

– обоснование состава и описание дизайна процедур тестирования;

– подготовка условий симуляции и/или натурных испытаний; определение порядка тестирования и накопления данных результатов испытаний;

– определение порядка обработки и оценки результатов испытаний; описание механизма обратной связи и улучшений процедур тестирования; формирование заключений и рекомендаций [18, 34 и др.].

Спецификация задач и схемы процесса тестирования позволяют определять и уточнять временные и стоимостные параметры разработки проекта испытательного полигона (состав и характеристики элементов, состав и характеристики оборудования, состав и график работ, объем и структура финансирования и др.), что схематично представлено на рис. 1.

Выводы

Подводя итоги выполненного исследования, можно сформулировать ряд выводов, имеющих принципиальное значение при разработке и создании надежных и безопасных технических решений в сфере CAD.

1. Стратегии развития технологий и систем CAV встраиваются в общую логику развития национальных транспортных систем[20] с учетом интеллектуализации инфраструктуры и сервисов, а также определения приоритетов в области безопасности эксплуатации высокоавтоматизированных транспортных средств.

2. Создание испытательного полигона для оценки состояния и обоснованию мер информационной безопасности системы взаимодействия «беспилотное транспортное средство — дорожная инфраструктура», представляет собой сложный комплексный проект, предполагающий участие представителей различных сторон: государства, бизнеса и науки.

3. Успешная реализации проекта зависит, прежде всего, от корректного определения целей тестирования информационной безопасности технологической платформы V2X и дифференциации задач тестирования для спецификации требований к полигону и реализации плана испытаний отдельных функций системы автоматизированного вождения и CAV в целом в условиях среды сетевых коммуникаций.

4. Необходима синхронизация планирования и осуществления технических работ проекта с разработкой мер нормативного правового регулирования создания и эксплуатации CAV: технологические требования и стандарты (регламенты и протоколы, законодательные нормы и правила (законы и подзаконные акты).

5. Дорожная карта создания испытательного полигона для оценки информационной безопасности платформы V2X должна формироваться как проект создания специализированной тестовой площадки для лабораторных и полевых испытаний на ограниченной территории с виртуаль-

[20] С учетом пространственной организации дорожной сети на огромной территории Российской Федерации важно распределение ответственности участников рынка, чтобы обеспечить баланс экономической и социальной эффективности программ создания национальной ИТС (на значительных участках трасс объем трафика обмена данными далек от требований рентабельности услуг мобильной связи).

ной и реальной имитацией дорожной сети и ситуаций в соответствии с разрабатываемой картой и моделью угроз для коммуникации CAV.

6. Порядок и правила тестирования информационной безопасности платформы V2X зависимы от регламента использования спектра частот сетями связи общего и специального назначения, что требует дополнительного согласования частотных характеристик и параметров используемого оборудования (особенно, если предполагается испытание зарубежных устройств и технологий, не используемых в настоящее время на территории России).

Таким образом, обеспечение необходимого уровня информационной безопасности является одной из ключевых задач обеспечения транспортной безопасности в целом. С ростом автоматизации транспортных средств, развитием их автономности требуется усилить работу по выявлению и изучению новых угроз. На наш взгляд, такая работа должна быть организована централизовано и подчиняться единому регламенту испытаний для оценки рисков эксплуатации CAV в среде ИТС. Такой регламент должен опираться на группу стандартов, которые необходимо разработать и постоянно совершенствовать.

Необходимо отметить, что в силу специфики отрасли тестирование и сертификацию необходимо проводить не только при разработке *новой* продукции, но и при периодическом контроле допуска ВАТС к эксплуатации, в том числе при подключении к сервисам ИТС. Это должно обеспечить повышение уровня безопасности пассажиров, исключить возможность или минимизировать вероятность появления инцидентов, приводящих к причинению вреда здоровью или материальному ущербу.

Представленные положения и сформулированные рекомендации могут быть полезны при разработке концепции и инструментария тестирования технологической платформы V2X. В правовом поле Российской Федерации необходимо описание требований к проектированию и созданию специализированного полигона для тестирования технологий обеспечения информационной безопасности систем автоматизированного вождения транспортных средств в различных условиях состояния сетевой инфраструктуры. Очевидной становится задача совершенствования нормативного регулирования[21] в области разработки и эксплуатации автоматизированного автомобильного транспорта различного типа, а также проведения сертификации систем и устройств ВАТС с позиции оценки информационной безопасности. Таким образом, одним из приоритетных направлений дальнейших исследований становятся разработка аппаратно-программных решений и технологических регламентов (стандартов) для обеспечения информационной безопасности, а также обоснование методики и создание инструментария тестирования беспилотных автомобилей различного назначения. Это позволит синхронизировать национальную повестку создания технологий беспилотного транспорта с общемировыми тенденциями построения инфраструктуры ИТС, ориентированной на решение задач стратегического развития Российской Федерации в условиях процесса цифровой трансформации общества, экономики и бизнеса.

СПИСОК ЛИТЕРАТУРЫ

1. **Sadrpour A., Jin J. et al.** Simulation-based acceptance testing for unmanned ground vehicles. International Journal of Vehicle Autonomous Systems, 2013, no. 11–1, pp. 62–85.

2. **Zou B., Li W., Wang D.** Analysis on current situation of China's intelligent connected vehicle road test regulations. MATEC Web of Conferences, 2019, no. 259, 02003. DOI: 10.1051/matecconf/201925902003

3. **Чучаев А.И., Маликов С.В.** Ответственность за причинение ущерба высокоавтоматизированным транспортным средством: состояние и перспективы // Актуальные проблемы российского права. 2019. № 6. С. 117–124.

[21] Включая коррекцию и адаптацию комплекса предварительных национальных стандартов Российской Федерации, разработанных техническим комитетом ТК 57 «Интеллектуальные транспортные системы» с учетом основных нормативных положений международных стандартов (ISO в области ИТС).

4. **Taeihagh A., Lim H.** Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transport Reviews, 2018, no. 39–1, pp. 103–128. DOI: 10.1080/01441647.2018.1494640

5. **Maurer M, Gerdes J. et al.** Autonomous driving. Technical, legal and social aspects. Springer, 2016. 706 p.

6. **Popkova E.G., Ostrovskaya V.N. (Eds.).** Perspectives on the use of new information and communication technology (ICT) in the modern economy. Springer, 2019. 1178 p.

7. **Носов А.Г.** Экономические и инфраструктурные аспекты развития технологий беспилотного транспорта // Транспорт Российской Федерации. 2016. № 5. С. 21–25.

8. **Казанская Л.Ф., Савицкая Н.В., Камзол П.П.** Перспективы развития беспилотного транспорта в России // Бюллетень результатов научных исследований. 2018. № 2. С. 18–28.

9. **Anderson J., Kalra N. et al.** Autonomous vehicle technology: A guide for policymakers. Santa Monica, CA, RAND Corporation. 2016. 214 p.

10. **Childress S., Nichols B. et al.** Using an activity-based model to explore possible impacts of automated vehicles. Journal of the Transportation Research Board, 2016, no. 2493, pp. 99–106.

11. **Schwab K.** The fourth industrial revolution. New York, Crown Business, 2017. 192 p.

12. **Чикрин Д.Е., Савенков П.А., Шагиев Р.И.** Интегрированные системы высокоточной спутниково-локально-инерциальной навигации в задачах беспилотного управления транспортными средствами // Наноиндустрия. 2019. № 5(89). С. 49–56.

13. **Иванов В.В., Малинецкий Г.Г.** Цифровая экономика: мифы, реальность, перспектива. М.: Российская академия наук, 2017. 63 с.

14. **Clements L., Kockelman K.** Economic effects of automated vehicles. Transportation Research Record Journal of the Transportation Research Board, 2017, no. 1, pp. 106–114.

15. **Дубинина М.Г., Макарова Ю.А.** Анализ технико-экономических показателей беспилотных транспортных средств // Концепции. 2018. № 1. С. 28–44.

16. **Ларин О.Н., Куприяновский В.П.** Вопросы трансформации рынка транспортно-логистических услуг в условиях цифровизации экономики. International Journal of Open Information Technologies. 2018. № 3. С. 95–101.

17. **Степанян А.Ж.** Проблемы регулирования беспилотных транспортных средств. Вестник Университета имени О.Е. Кутафина, 2019. № 4(56). С. 169–174. DOI: 10.17803/2311-5998.2019.56.4.169-174

18. Automotive security: Best practices. Recommendations for security and privacy in the era of the next-generation car. McAfee White paper, 2016. 23 p.

19. **Zhao D., Lam H. et al.** Accelerated evaluation of automated vehicles safety in lane-change scenarios based on importance sampling techniques. IEEE Transactions on Intelligent Transportation Systems, no. 18–3, pp. 595–607. DOI: 10.1109/TITS.2016.2582208

20. **Cui J., Sabaliauskaite G.** On the alignment of safety and security for autonomous vehicles. Proc. IARIA CYBER 2017. Barcelona, 2017, pp. 1–6.

21. **Schneier B.** Secrets and lies: Digital security in a networked world. Wiley, 2015. 448 p.

22. **Лахметкина Н.Ю., Щелкунова И.В., Рогова Д.А.** Развитие транспортных систем в цифровой повестке // Интеллект. Инновации. Инвестиции. 2019. № 4. С. 114–120.

23. **Tokody D., Albini A. et al.** Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city. Interdisciplinary Description of Complex Systems, 2018, no. 16(3-A), pp. 384–396. DOI: 10.7906/indecs.16.3.11

24. **Checkoway S., McCoy D. et al.** Comprehensive experimental analyses of automotive attack surfaces. Proceedings of the 20th USENIX conference on Security (SEC'11). 2011, 6.

25. **Miller C., Valasek C.** A survey of remote automotive attack surfaces. Black Hat, 2014. 94 p.

26. **Szalay Z., Tettamanti T. et al.** Development of a test track for driverless cars: Vehicle design, track configuration, and liability considerations. Periodica Polytechnica Transportation Engineering, 2018, no. 46(1), pp. 29–35. DOI: 10.3311/PPtr.10753

27. **Montremerlo M., Beeker J. et al.** The Stanford entry in the urban challenge. Journal of Field Robotics, 2008, no. 7(9), pp. 468–492.

28. **Chen R., Arief M. et al.** How to evaluate proving grounds for self-driving? A quantitative Approach. arXiv preprint, 2020, 1909.09079v5. URL: https://arxiv.org/pdf/1909.09079.pdf (дата обращения: 10.08.2020)

29. **Chen R., Arief M., Zhao D.** An "Xcity" optimization approach to designing proving grounds for connected and autonomous vehicles. arXiv preprint, 2018, 1808.03089v1. URL: https://arxiv.org/pdf/1808.03089.pdf (дата обращения: 10.08.2020)

30. **Szalay Z., Nyerges A. et al.** Technical specification methodology for an automotive proving ground dedicated to connected and automated vehicles. Periodica Polytechnica Transportation Engineering, 2017, no. 45(3), pp. 168–174. DOI: 10.3311/PPtr.10708

31. **Huang W., Wang K. et al.** Autonomous vehicles testing methods review. IEEE 19th International Conference on Intelligent Transportation Systems, 2016, pp. 163–198. DOI: 10.1109/ITSC.2016.7795548

32. **Joerger M., Jones C., Shuman V.** Testing connected and automated vehicles (CAVs): Accelerating innovation, integration, deployment and sharing results. Meyer G., Beiker S. (Eds.). Road vehicles automation. 5th ed. Springer, 2019, pp. 197–206.

33. **Geiger A., Lenz P., Urtasun R.** Are we ready for autonomous driving? The KITTI vision benchmark suite. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2012, pp. 3354–3361. DOI: 10.1109/CVPR.2012.6248074

34. **Huang W., Wen D. et al.** Task-specific performance evaluation of UGV's: Case studies at the IVFC. IEEE Transactions on Intelligent Transportation Systems, 2014, no. 15(5), pp. 1969–1979.

REFERENCES

1. **A. Sadrpour, J. Jin, et al.,** Simulation-based acceptance testing for unmanned ground vehicles. International Journal of Vehicle Autonomous Systems, 2013, no. 11–1, pp. 62–85.

2. **B. Zou, W. Li, D. Wang,** Analysis on current situation of China's intelligent connected vehicle road test regulations. MATEC Web of Conferences, 2019, no. 259, 02003. DOI: 10.1051/matecconf/201925902003

3. **A.I. Chuchaev, S.V. Malikov,** Otvetstvennost za prichineniye ushcherba vysokoavtomatizirovannym transportnym sredstvom: sostoyaniye i perspektivy [Liability for causing damage by a highly automated vehicle: state and prospects]. Aktualnyye problemy rossiyskogo prava, 2019, no. 6, pp. 117–124. (rus)

4. **A. Taeihagh, H. Lim,** Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transport Reviews, 2018, no. 39–1, pp. 103–128. DOI: 10.1080/01441647.2018.1494640

5. **M. Maurer, J. Gerdes, et al.,** Autonomous driving. Technical, legal and social aspects. Springer, 2016. 706 p.

6. **E.G. Popkova, V.N. Ostrovskaya (Eds.),** Perspectives on the use of new information and communication technology (ICT) in the modern economy. Springer, 2019. 1178 p.

7. **A.G. Nosov,** Ekonomicheskiye i infrastrukturnyye aspekty razvitiya tekhnologiy bespilotnogo transporta [Economic and infrastructural aspects of the development of technologies for unmanned vehicles]. Transport Rossiyskoy Federatsii, 2016, no. 5, pp. 21–25. (rus)

8. **L.F. Kazanskaya, N.V. Savitskaya, P.P. Kamzol,** Perspektivy razvitiya bespilotnogo transporta v Rossii [Prospects for the development of unmanned vehicles in Russia]. Byulleten rezultatov nauchnykh issledovaniy, 2018, no. 2, pp. 18–28. (rus)

9. **J. Anderson, N. Kalra, et al.,** Autonomous vehicle technology: A guide for policymakers. Santa Monica, CA, RAND Corporation. 2016. 214 p.

10. **S. Childress, B. Nichols, et al.,** Using an activity-based model to explore possible impacts of automated vehicles. Journal of the Transportation Research Board, 2016, no. 2493, pp. 99–106.

11. **K. Schwab,** The fourth industrial revolution. New York, Crown Business, 2017. 192 p.

12. **D.E. Chikrin, P.A. Savenkov, R.I. Shagiev,** Integrirovannyye sistemy vysokotochnoy sputnikovo-lokalno-inertsialnoy navigatsii v zadachakh bespilotnogo upravleniya transportnymi sredstvami [Integrated systems of high-precision satellite-local-inertial navigation in the tasks of unmanned vehicle control]. Nanoindustriya, 2019, no. 5(89), pp. 49–56. (rus)

13. **V.V. Ivanov, G.G. Malinetskiy,** Tsifrovaya ekonomika: mify, realnost, perspektiva [Digital economy: Myths, reality, perspective]. Moscow, Rossiyskaya akademiya nauk, 2017. 63 p. (rus)

14. **L. Clements, K. Kockelman,** Economic effects of automated vehicles. Transportation Research Record Journal of the Transportation Research Board, 2017, no. 1, pp. 106–114.

15. **M.G. Dubinina, Yu.A. Makarova,** Analysis of technical and economic characteristics of unmanned transport vehicles. Concepcii, 2018, no. 1, pp. 28–44. (rus)

16. **O.N. Larin, V.P. Kupriyanovskiy,** Voprosy transformatsii rynka transportno-logisticheskikh uslug v usloviyakh tsifrovizatsii ekonomiki [Transformation of the market of transport and logistics services in the context of digitalization of the economy]. International Journal of Open Information Technologies, 2018, no. 3, pp. 95–101. (rus)

17. **A.Z. Stepanian,** Problems of regulation of unmanned vehicles. Courier of Kutafin Moscow State Law University, 2019, no. 4, pp. 169–174. (rus). DOI: 10.17803/2311-5998.2019.56.4.169-174

18. Automotive security: Best practices. Recommendations for security and privacy in the era of the next-generation car. McAfee White paper, 2016. 23 p.

19. **D. Zhao, H. Lam, et al.,** Accelerated evaluation of automated vehicles safety in lane-change scenarios based on importance sampling techniques. IEEE Transactions on Intelligent Transportation Systems, no. 18–3, pp. 595–607. DOI: 10.1109/TITS.2016.2582208

20. **J. Cui, G. Sabaliauskaite,** On the alignment of safety and security for autonomous vehicles. Proc. IARIA CYBER 2017. Barcelona, 2017, pp. 1–6.

21. **B. Schneier,** Secrets and lies: Digital security in a networked world. Wiley, 2015. 448 p.

22. **N.U. Lakhmetkina, I.V. Schelkunova, D.A. Rogova,** The development of transport systems in the digital agenda. Intelligence. Innovations. Investment, 2019, no. 4, pp. 114–120. (rus.). DOI: 10.25198/2077-7175-2019-4-114

23. **D. Tokody, A. Albini, et al.,** Safety and security through the design of autonomous intelligent vehicle systems and intelligent infrastructure in the smart city. Interdisciplinary Description of Complex Systems, 2018, no. 16(3-A), pp. 384–396. DOI: 10.7906/indecs.16.3.11

24. **S. Checkoway, D. McCoy, et al.,** Comprehensive experimental analyses of automotive attack surfaces. Proceedings of the 20th USENIX conference on Security (SEC'11). 2011, 6.

25. **C. Miller, C. Valasek,** A survey of remote automotive attack surfaces. Black Hat, 2014. 94 p.

26. **Z. Szalay, T. Tettamanti, et al.,** Development of a test track for driverless cars: Vehicle design, track configuration, and liability considerations. Periodica Polytechnica Transportation Engineering, 2018, no. 46(1), pp. 29–35. DOI: 10.3311/PPtr.10753

27. **M. Montremerlo, J. Beeker, et al.,** The Stanford entry in the urban challenge. Journal of Field Robotics, 2008, no. 7(9), pp. 468–492.

28. **R. Chen, M. Arief, et al.,** How to evaluate proving grounds for self-driving? A quantitative Approach. arXiv preprint, 2020, 1909.09079v5. URL: https://arxiv.org/pdf/1909.09079.pdf (accessed August 10, 2020)

29. **R. Chen, M. Arief, D. Zhao,** An "Xcity" optimization approach to designing proving grounds for connected and autonomous vehicles. arXiv preprint, 2018, 1808.03089v1. URL: https://arxiv.org/pdf/1808.03089.pdf (accessed August 10, 2020)

30. **Z. Szalay, A. Nyerges, et al.,** Technical specification methodology for an automotive proving ground dedicated to connected and automated vehicles. Periodica Polytechnica Transportation Engineering, 2017, no. 45(3), pp. 168–174. DOI: 10.3311/PPtr.10708

31. **W. Huang, K. Wang, et al.,** Autonomous vehicles testing methods review. IEEE 19th International Conference on Intelligent Transportation Systems, 2016, pp. 163–198. DOI: 10.1109/ITSC.2016.7795548

32. **M. Joerger, C. Jones, V. Shuman,** Testing connected and automated vehicles (CAVs): Accelerating innovation, integration, deployment and sharing results. Meyer G., Beiker S. (Eds.). Road vehicles automation. 5th ed. Springer, 2019, pp. 197–206.

33. **A. Geiger, P. Lenz, R. Urtasun,** Are we ready for autonomous driving? The KITTI vision benchmark suite. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2012, pp. 3354–3361. DOI: 10.1109/CVPR.2012.6248074

34. **W. Huang, D. Wen, et al.,** Task-specific performance evaluation of UGV's: Case studies at the IVFC. IEEE Transactions on Intelligent Transportation Systems, 2014, no. 15(5), pp. 1969–1979.

Статья поступила в редакцию 02.09.2020.

СВЕДЕНИЯ ОБ АВТОРАХ / THE AUTHORS

ПИСАРЕВА Ольга Михайловна
E-mail: o.m.pisareva@gmail.com
PISAREVA Olga M.
E-mail: o.m.pisareva@gmail.com

АЛЕКСЕЕВ Вячеслав Аркадьевич
E-mail: vaalexeev@gmail.com
ALEXEEV Vyacheslav A.
E-mail: vaalexeev@gmail.com

МЕДНИКОВ Дмитрий Николаевич
E-mail: dn_mednikov@guu.ru
MEDNIKOV Dmitry N.
E-mail: dn_mednikov@guu.ru

СТАРИКОВСКИЙ Андрей Викторович
E-mail: av_starikovskiy@guu.ru
STARIKOVSKY Andrey V.
E-mail: av_starikovskiy@guu.ru