DOI: 10.18721/JE.14402
УДК 338.47 : 330.47 : 656.13 : 004.056

ХАРАКТЕРИСТИКА ЗОН УЯЗВИМОСТИ И ИСТОЧНИКОВ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭКСПЛУАТАЦИИ БЕСПИЛОТНЫХ АВТОМОБИЛЕЙ В ИНТЕЛЛЕКТУАЛЬНОЙ ТРАНСПОРТНОЙ СИСТЕМЕ

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

Полномасштабное развертывание интеллектуальных транспортных систем с транспортными средствами автоматизированного движения и связанной дорожной инфраструктурой в урбанизированных пространствах открывает не только дополнительные перспективы роста эффективности отрасли перевозок, но и ведет к появлению дополнительных источников угроз, рисков и зон уязвимости таких систем. При расширении состава различного рода угроз нарушения штатного функционирования беспилотного автомобильного транспорта (CAV), включая воздействия на каналы информационного взаимодействия всех участников дорожного движения и элементов дорожной инфраструктурой в рамках интеллектуальной транспортной системы (ITS), требуется дальнейшее совершенствование норм и требований правового и технического регулирования создания и эксплуатации CAV. Это расширение области и задач тестирования безопасности автомобильного общественного, личного, коммерческого и специального транспорта, в том числе за счет проверки информационной безопасности при валидации и верификации как CAV, так и компонентов ITS. В рамках системного подхода с использованием методов контентного, логического и сравнительного анализа проведено уточнение предметной области исследования, охарактеризовано состояние нормативных требований национальных регуляторов по обеспечению информационной безопасности подключенных и автоматизированных транспортных средств, рассмотрены методические подходы по тестированию по информационной безопасности автоматизированного дорожного движения в рамках интеллектуальной транспортной системы. В работе представлен концептуальный подход к идентификации комплексной модели угроз для информационной безопасности технологической платформы информационного взаимодействия «беспилотное транспортное средство-дорожная инфраструктура». Проведенное исследование на основе анализа требований безопасности для беспилотных автомобилей и уточнения понятий в сфере обеспечения информационной безопасности эксплуатации CAV и функционирования ITS в условиях перехода к мобильной связи поколения 5G позволило получить следующие результаты: определить состав типовых зон уязвимостей и потенциальных атак; охарактеризовать спектр основных угроз, классифицировать основных агентов угроз информационной безопасности в архитектуре CAV и инфраструктуре ITS. Прикладное значение полученных результатов исследования состоит в возможности использования представленной модели угроз информационной безопасности CAV при разработке методических подходов и аналитических инструментов для организации и тестирования в рамках лабораторных экспериментов и полигонных испытаний различных видов преднамеренных нарушений каналов информационного взаимодействия отдельных устройств CAV, группы автономных транспортных средств и отдельного CAV с ITS. После закрепления нормативных требований в отечественном стандарте информационной безопасности CAV возможным направлением дальнейших исследований может стать разработка технологической и экономической моделей тестирования информационной безопасности в рамках ITS для национальной системы сертификации CAV различного типа.

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

Ссылка при цитировании: Писарева О.М., Алексеев В.А., Медников Д.Н., Стариковский А.В. Характеристика зон уязвимости и источников угроз информационной безопасности эксплуатации беспилотных автомобилей в интеллектуальной транспортной системе // Научно-технические ведомости СПбГПУ. Экономические науки. 2021. Т. 14, № 4. С. 20–36. DOI: 10.18721/JE.14402

CHARACTERISTICS OF VULNERABILITY ZONES AND SOURCES OF THREATS FOR INFORMATION SECURITY FROM THE OPERATION OF UNMANNED VEHICLES IN AN INTELLIGENT TRANSPORT SYSTEM

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

The full-scale deployment of intelligent transport systems with automated vehicles and associated road infrastructure in urbanized spaces opens up additional prospects for increasing the efficiency of the transportation industry. However, it also leads to the emergence of additional sources of threats, risks and areas of vulnerability of such systems. The range of various kinds of threats disrupting the normal functioning of connected and automated vehicles (CAV) is expanding. It includes the impact of the interaction between all road users and elements of the road infrastructure on the channels of information within the framework of the intelligent transport system (ITS). There is a growing need for further improvement of the norms and requirements of legal and technical regulation of CAV production and operation. It means an expansion of the field and tasks of testing the safety of public, personal, commercial and special automobile vehicles, including through the verification of information security during the validation and verification of both CAV and ITS components. The authors employed a systematic approach using methods of content, logical and comparative analysis in the research. The paper clarifies the subject area of the study, characterizes the state of national regulators' requirements for ensuring information security of connected and automated vehicles, and considers methodological approaches to testing information security of automated road traffic within the framework of intelligent transport systems. The authors present a conceptual approach to the identification of a complex model of threats to information security of the technological platform of information interaction "unmanned vehicle-road infrastructure". The study was based on the analysis of security requirements for unmanned vehicles and clarification of concepts in the field of information security for the operation of CAV and the functioning of ITS in the transition to mobile communications of the 5G generation. The main results of the research include the composition of typical zones of vulnerabilities and potential attacks; characteristics of the spectrum of the main threats; classification of the main agents of information security threats in the CAV architecture and ITS infrastructure. The applied value of the obtained results lies in the possibility of using the presented model of CAV information security threats in the development of methodological approaches and analytical tools for organizing and testing various types of deliberate violations of communication channels of individual CAV devices, a group of autonomous vehicles and a separate CAV with ITS in the framework of laboratory experiments and field tests. After the regulatory requirements are formalized in the national CAV information security standard, a possible direction for further research may be the development of technological and economic models for testing information security within the framework of ITS for the national certification system CAV of various types.

Keywords: digital technologies, information security, unmanned vehicles, test site, intelligent transportation system

Citation: O.M. Pisareva, V.A. Alexeev, D.N. Mednikov, A.V. Starikovsky. Characteristics of vulnerability zones and threats sources for information security by the operation of unmanned vehicles in an intelligent transport system, St. Petersburg State Polytechnical University Journal. Economics, 14 (4) (2021) 20–36. DOI: 10.18721/JE.14402

Введение

Одним из экономически значимых следствий цифровой трансформации экономики, имеющим и социальные последствия, является расширяющееся внедрение подключенных и автоматизированных транспортных средств (АТС), включая автомобильные (Connected Automated Vehicles, CAV). С переходом к мобильной связи следующего поколения 5G (а также модернизацией решений с использованием протоколов коммуникаций в формате LTE) появилась возможность построения единой технологической платформы высокоскоростного обмена электронными данными и применения методов искусственного интеллекта в общей цифровой среде между автомобилем и различными элементами внешнего окружения в целостной транспортной системе (Vehicle-to-Everything, V2X). Все это является важнейшим шагом для полномасштабного развертывания интеллектуальных транспортных систем (Intelligent Transportation Systems, ITS) с транспортными средствами автоматизированного движения (Automated Driving, AD) и связанной дорожной инфраструктуры в урбанизированных пространствах с сетью дорог различной плотности и назначения: открытые (магистрали и шоссе), городские (улицы и переулки) и ограниченные (специальные хозяйственные и общественные зоны) участки территорий стран. Создание национальной ITS предполагает решение широкого круга задач в технической и экономической, организационной и правовой сферах организации беспилотного движения автомобильного транспорта. Для реализации функциональных возможностей CAV в цифровой экономике должны быть изучены и решены вопросы обеспечения безопасности их эксплуатации, в том числе и прежде всего в области информационной безопасности инновационных решений для беспилотных автомобилей личного и коммерческого, общественного и специального назначения, дорожной инфраструктуры, а также систем организации и регулирования дорожного движения.

Цель исследования

Объектом настоящего исследования является транспортная отрасль Российской Федерации. Предмет исследования – обеспечение информационной безопасности эксплуатации беспилотных автомобилей в интеллектуальной транспортной системе.

Главная цель исследования состоит в определении подходов к выявлению и анализу зон уязвимости и источников угроз информационной безопасности подключенных, автоматизированных и автоматических транспортных средств при организации процесса их проектирования, разработки, создания (производства) и эксплуатации.

Основные задачи исследования, предопределенные содержанием общей проблемы обеспечения безопасности дорожного движения и логикой государственного регулирования технологического развития транспортной системы, заключаются в определении и характеристике состава элементов технологической платформы CAV-ITS, подверженным угрозам информационной безопасности, а также в идентификации и классификации источников угроз информационной безопасности и способов их реализации в цифровой среде информационного и коммуникационного обеспечения эксплуатации беспилотных автомобилей. Результаты решения указанных задач создают предпосылки для системного и согласованного рассмотрения проблем практической реализации возможностей беспилотного транспорта в части определения предмета и функций задач тестирования уровня информационной безопасности создаваемых и выводимых на рынок транспортных услуг технологических платформ интеграции автономного автомобиля и дорожной инфраструктуры, которые должны быть отражены при обосновании ключевых принципов и требований нормативного регулирования создания национальной интеллектуальной транспортной системы и технической сертификации беспилотных автомобилей.

Методика

Достижение поставленной цели и решение сформулированных задач исследования предполагает применение комплекса общенаучных методов контентного и сравнительного, логического и системного анализа для изучения отечественного и зарубежного опыта разработки и внедрения технологий CAV, для обобщения сложившейся законодательной практики регулирования информационной безопасности эксплуатации CAV на выделенных участках дорожной сети и дорогах общего пользования, для характеристики подходов тестирования информационной безопасности технологической платформы CAV-ITS в условиях стендовых (лабораторных) и полевых (полигонных) испытаний беспилотных автомобилей. При анализе и решении комплекса проблем обеспечения информационной безопасности CAV авторы предлагают использовать оригинальный методический подход, заключающийся во взаимосвязанном рассмотрении ключевых особенностей конструкции беспилотного автомобиля и архитектуры интеллектуальной дорожной инфраструктуры на технологической платформе V2X как концептуальный основы формирования профиля рисков и оценки рисков CAV, обусловленных различными способами нарушения контура информационной защиты в среде ITS. Источниками информации стали доступные открытые публикации научного и экспертного характера, аналитические материалы научных и исследовательских центров разработки технологий и оборудования для ITS, официальные правовые документы и статистические данные о разработке, тестировании и внедрении CAV с обеспечением информационной безопасности их эксплуатации для национальных и международных челночных и магистральных перевозок грузов и пассажиров.

Результаты и обсуждение

Внедрение технологий беспилотного транспорта оказывает возрастающее и расширяющееся влияние на социально-экономическое развитие передовых стран, что сопровождается появлением нового спектра институциональных и технических проблем регулирования создания и сертификации беспилотных автомобилей с различным уровнем автоматизации движения, включая проверку обеспечения требований информационной безопасности.

Инновации в автомобилях и дорожной сети следующего поколения, связаны, прежде всего, с расширением возможности сетевого подключения, для чего промышленность уже внедрила или готова внедрить (при решении смежных правовых и организационных вопросов ITS) новые функции. Эти инновационные функции часто называют «киберфизическими», поскольку почти все они требуют сбора данных о транспортной киберсистеме из физической и цифровой сфер описания внутренней (состояние транспортного средства) и внешней (состояние окружения) среды для принятия решений о дальнейшей эксплуатации автомобилей и выполнения таких решений с физическими последствиями. Общая схема экосистемы и инфраструктура подключенного и автономного транспортного средства представлена на рис. 1.

Анализ национальных и межгосударственных стратегий развития автоматизированного движения, показывает, что одним из ключевых моментов организации широкого развертывания и эффективного использования подключенных и автономных транспортных средств является проведение исследований и разработок в области построения интеллектуальных транспортных систем. Отраслевые эксперты обозначают критическое значение и определяют ведущую роль вопроса обеспечения безопасности CAV при их масштабном встраивании в процессы общественных, коммерческих и персональных перевозок, включая решение задачи *безопасности* (Cyber Security) для информационного взаимодействия беспилотного автомобиля (БА) с дорожной инфраструктурой (ДИ) в рамках ITS.

Оценка и сопоставление различных подходов к определению безопасного состояния CAV позволяет определить перечень требований безопасности для беспилотного автомобильного транспорта [1] в части понимания состояния его:

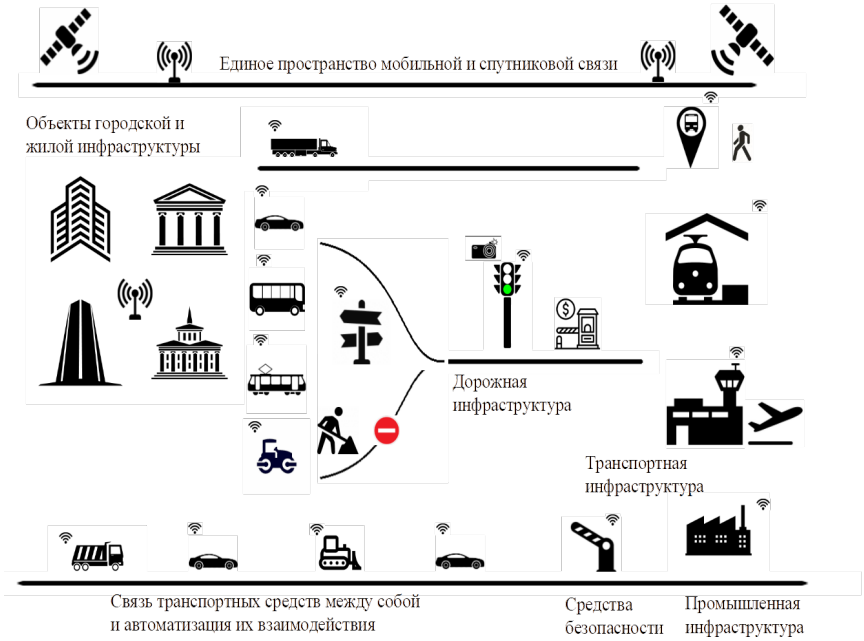

Рис. 1. Схематичное представление экосистемы высокоавтоматизированного транспортного средства

Схематичное представление экосистемы высокоавтоматизированного транспортного средства[1]

Fig. 1. Schematic representation of the ecosystem for highly automated vehicles

– текущих эксплуатационных возможностей;

– текущих функциональных ограничений по отношению к сложившейся ситуации;

– предельных возможностей эксплуатации в условиях, когда уровень риска является приемлемым для пассажиров и транспортируемого груза и других участников дорожного движения;

– безопасности и минимизации помех движению при остановке на обочине или возле тротуара;

– безопасности при нахождении в полосе движения только при соблюдении всех следующих условий: относительная скорость для других участников дорожного движения ниже максимальной; стационарное транспортное средство не блокирует маршруты доступа аварийных транспортных средств или путей аварийного выхода; в течение короткого времени автомобиль может быть выведен водителем-контролером или удаленным оператором с полосы движения; водитель-контролер может защитить автомобиль от различных угроз;

– зон риска и степени уязвимости в условиях движения или опасного местонахождения (например, остановка в опасном месте), безусловно инициирующих отправление аварийного сигнала и запрос помощи.

Охарактеризуем события, связанные с безопасностью. В дорожном движении могут происходить различные события, которые влияют на риски негативного развития текущей ситуации и в ближайшем будущем. С одной стороны, технические дефекты и неисправности в системе управления транспортного средства снижают его эксплуатационные качества, а с другой, изменения условий окружающей среды, ситуации, которые перегружают систему управления транспортного средства, неправильное поведение других участников дорожного движения и форс-мажорные обстоятельства увеличивают требования к системе управления транспортным средством. В частности, сочетание сниженных возможностей управления и повышенного количества внешних факторов приводит к повышению уровня риска ДТП. Дефекты и технические неисправности на транспортном средстве и в системе его наведения могут возникать внезапно, и поэтому их очень трудно предвидеть. Помимо механических дефектов на транспортном

[1] См.: White paper. Automotive Security: Best Practices. Recommendations for security and privacy in the era of the next-generation car. McAfee. 2016.

средстве, дефекты и ошибки разработки в системе наведения транспортного средства могут привести к снижению эксплуатационных характеристик. Неблагоприятные условия освещения и погодные условия повышают требования к долговечности датчиков, используемых для контроля окружающей среды и дорожной обстановки. Кроме того, неблагоприятные погодные условия приводят к ухудшению дорожных условий. Это напрямую влияет на динамику вождения. Из-за сложности дорожного движения и бесконечного количества возможных ситуаций, вероятно, что не все ситуации будут приняты во внимание при разработке системы управления транспортным средством. Если транспортное средство сталкивается с ситуацией, которая не может быть разрешена с помощью существующего программного обеспечения, это напрямую влияет на уровень риска негативного развития ситуации. Отдельного изучения требует поведение нескольких CAV с различным программным обеспечением. Поведение других участников дорожного движения не всегда соответствует правилам, и может случиться так, что их нестандартное поведение является отдельным источником опасного поведения CAV. В некоторых ситуациях эксплуатация автоматизированного транспортного средства никогда не может быть безопасной, поскольку другие участники дорожного движения действуют опасным образом. В таких ситуациях признанные ограничения возможностей автоматизированного транспортного средства и средств управления движением является сложной задачей при создании интеллектуальной транспортной системы. Форс-мажорные обстоятельства могут также представлять отдельную угрозу, приводящую к повышению риска эксплуатации, например, из-за землетрясений, внезапных наводнений или солнечных вспышек, которые приводят к помехам в используемых системах, таких как глобальная спутниковая навигационная система или связь между транспортными средствами [2]. При этом в соответствии с ISO 26262 [3] подобные события не учитываются при разработке систем помощи при вождении.

Таким образом, 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, взаимодействующих между собой киберфизических систем, приводит к повышению рисков автономного / автоматизированного движения транспортных средств. Поэтому разработка технологий управления CAV нуждается в оценке последствий использования, что требует комплексного моделирования структуры взаимосвязей в киберфизических системах интеллектуального автомобильного транспорта. Механизм взаимодействия/связи автоматизированного или автономного интеллектуального транспортного средства с физической и киберфизической инфраструктурой формируется под влиянием широкого внедрения ключевых обеспечивающих технологий интеллектуальной мобильности (Key Enabling Technologies of Smart Mobility): автоматизации движения; цифрового интерфейса; цифровых данных; информационной взаимосвязанности, которые подробно рассматриваются, например, в работе [4].

Очевидно, что эффективно обеспечить безопасность эксплуатации CAV и функционирования ITS в целом нельзя, имея дело с отдельными компонентами, угрозами или точками атаки. Учитывая природу рассматриваемой киберфизической системы, определяющим аспектом здесь, конечно, является безопасность объединенной системы, которая состоит из системы управления CAV и системы управления дорожной инфраструктурой. Реализация соответствующих требований предполагает применение целостного системного подхода с оценкой участия и влияния отдельных элементов всей экосистемы автономного автомобильного транспорта. Во-первых, для киберфизических систем источник (фактор) риска может находиться и в реальном, и в виртуальном мире, во-вторых, последствия спровоцированных факторами риска инцидентов также происходят в реальном и виртуальном мире. Это существенно затрудняет защиту систем CAV, включая устройства и элементы технологической платформы информа-

ционного взаимодействия «высокоавтоматизированное транспортное средство-дорожная инфраструктура» (далее – ТП ВАТС-ДИ), а также предполагает качественное изменение подхода к построению и тестированию аппаратно-программных и информационно-технологических средств противодействия негативным информационным воздействиям (как умышленным атакам, так и случайным влияниям событий различного рода в киберфизической системе CAV и инфраструктуре ITS).

В соответствии с общей структурой стратегической модели киберфизических систем совокупность высокоавтоматизированных транспортных средств в среде интеллектуальной дорожной инфраструктуры, представленной в схожих подходах анализа целого ряда исследователей и экспертов (см., например, работы [1–4]) можно определить множество наиболее уязвимых для атаки элементов (поверхностей) высокоавтоматизированного транспортного средства и направлений (способов) воздействия на него. Так на рис. 2 показана схема расположения зон уязвимости для гипотетического представителя семейства CAV.

В ряде специальных исследовательских работ ранее проводился анализ уязвимости моделей транспортных средств с различным уровнем автоматизации [1, 5, 6, 7 и др.], в которых определена типология дистанционных атак в зависимости от трех категорий характеристик CAV:

– зоны для удаленной атаки;
– киберфизических особенностей транспортного средства;
– используемой сетевой архитектуры.

В частности, в работе [8] выделено семь основных категорий дистанционных атак, основанных на анализе характеристик 20 моделей транспортных средств. При этом была установлена четкая тенденция возрастания возможных потенциальных векторов атаки для более новых моделей автомобилей с технологиями CAV, 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 ITS (с желательным опережением характеристик перспективных/прогнозируемых методов взлома контура безопасности киберфизической системы CAV) [9, 10].

Охарактеризуем типологию нарушителей, формирующих угрозы кибербезопасности для CAV с характеристиками моделей и мотивов вредоносных действий (т.е. не случайных факторов), приведенную в обзоре [11]. В исследовании отмечается, что одним из наиболее важных шагов в улучшении состояния безопасности киберфизических систем в целом и автономных транспортных средств в частности, является понимание мотивов, целей и действий нарушителей или агентов угроз. Нарушители довольно разнообразны, но знание, кто они, моделирование их поведения, может помочь в планировании наиболее эффективных стратегий смягчения угроз и минимизации рисков. Возрастающая связность устройств сетевыми коммуникациями, с одной стороны, расширяет пространство угроз, увеличивает возможности атаки и, следовательно, увеличивает риск для подключенных к Интернету по различным протоколам устройств, включая беспилотные автомобили и элементы транспортной инфраструктуры. С другой стороны, появилась возможность накапливать и систематизировать обширные сведения об атаках с различными последствиями в виде неправильного поведения или отказа транспортного средства и транспортной инфраструктуры, что позволяет проводить всесторонний анализ инцидентов. Это позволило преодолеть исторически сложившуюся фрагментированность исследования масштаба, хронологии и характера предпринятых и реализованных попыток несанкционированных деструктивных действий в той или иной сфере подключенных устройств. В этой связи весьма успешной оказалась предпринятая компанией IT Threat Assessment Group (торговая марка McAfee®) разработка по идентификации и оценке угроз, в результате чего была создана библиотека агентов угроз [6] и модель использования оценки риска агентов угроз [7]. Так, на основе предпринятого анализа были выделены следующие пять групп агентов.

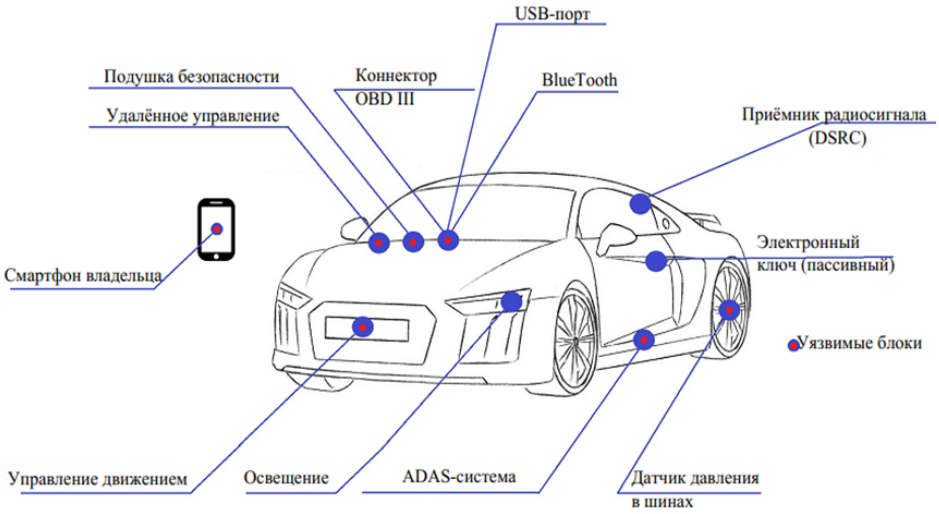

Рис. 2. Потенциальные направления атак и точки входа для взлома интеллектуальной системы управления высокоавтоматизированным транспортных средством

Источник: CRC[2]

Fig. 2. Potential attack directions and entry points for hacking the intelligent control system of highly automated vehicles

1) Исследователи и любители (Researchers and hobbyists). Их мотивы обычно положительны, и у них есть значительное время и доступ для проведения исследований. Задачи исследований часто предназначены для выявления уязвимостей, а результаты, как правило, свободно распространяются среди других пользователей для предотвращения угроз и внесения необходимых корректировок продуктов и сервисов. Хотя обмен информацией в тоже время доступен для потенциальных злоумышленников, преимущества информации об угрозах безопасности той или иной киберфизической системе и открывающаяся возможность корректирующих действий перевешивают сопутствующие риски.

2) Хакеры «любители» (Pranksters and hacktivists). Представители этой группы агентов угроз составляют негативную часть любителей, поскольку используют возможность продемонстрировать свои навыки с отрицательными результатами для владельца или производителя подключенного устройства. Количество «шутников» и причиняемый ими вред, как правило, ограничивается относительной сложностью используемых в автомобильной промышленности и транспортной сфере продуктов и устройств, способных при вмешательстве в зонах уязвимостей приводить к тем или иным потерям.

3) Владельцы и операторы (Owners and operators). Многие инструменты для взлома автомобилей доступны для владельцев различных подключенных устройств. Не являясь преступниками, эти люди потенциально могут иметь мотив «взломать» свои собственные транспортные средства для ремонта и технического обслуживания, чтобы, например, улучшить показатели производительности, снять ограничения, наложенные производителем или государственным регулятором, или отключить некоторые элементы системы, чтобы скрыть свои действия по личным или мошенническим причинам. Это может обернуться катастрофической проблемой для некоторых систем и устройств, являющихся критически важными для безопасности подключенного интеллектуального автомобиля. Следовательно, подобное несанкционированное вмешательство или модификации системы могут, в конечном итоге, также приводить к дорожно-транспортному

[2] CRC (The Congressional Research Service) – структурное подразделение Библиотеки Конгресса США (The Library of USA Congress), обеспечивающее экспертно-консультативную и информационно-аналитическую поддержку законотворческой и контрольной работы членов нижней палаты парламента США. В частности, при рассмотрении аспектов правового регулирования развития технологий CAV и обеспечения кибербезопасности им был подготовлен специальный обзорный отчет (см.: Canis B. Issues in Autonomous Vehicle Testing and Deployment (Updated November 27, 2019). CRS Report, R45985. Congressional Research Service, USA, 2019. 25 p.).

происшествию с той или иной степенью ответственности для нарушителя при установлении его причастности к причинам происшествия. Очевидно, что производитель подключенного транспортного средства заинтересован в ограничении подобных действий с помощью соответствующих функций безопасности, обеспечивая нормальный режим функционирования интеллектуальных систем и эксплуатации автомобиля и минимизируя свою дополнительною ответственность.

4) Организованная преступность (Organized crime). Оргпреступность всегда была угрозой для транспортных средств. В настоящее время она является серьезной угрозой и в сфере кибербезопасности. Основной мотивацией этой группы (зачастую, опережающей исследователей по своим техническим возможностям) является финансовая выгода, поэтому злоумышленники будут искать способы более легкого угона автомобилей и/или кражи транспортируемого груза. Киберугрозы часто следуют по эволюционной схеме, начиная с отказа в обслуживании (DoS), внедрения вредоносных программ, затем появления вымогателей и атак, направленных на определенные объекты. В этом случае DoS или отключение функций транспортного средства могут быть нацелены на конкретные модели транспортного средства, географические регионы, компании по аренде автомобилей и другие корпоративные автопарки. Вредоносные программы, следуя схожему образцу, могут вмешиваться в функционирование системы автоматизированного вождения и использовать различные внутренние данные о транспортном средстве (трафик, маршруты, груз, пробег, обслуживание, ремонт и т.п.), чтобы найти необходимые ценные сведения для криминального использования, в том числе для продажи персональной и конфиденциальной информации. В этом случае факт вымогательства может включать в себя удержание отдельных автомобилей (их парка) или в целом прерывание движения с целью создания хаоса для получения финансовой или политической выгоды. В области кибербезопасности эти инструменты атак стали использоваться и для такой модели киберпреступности, как оказание в интересах «заказчиков» специальных «услуг», потенциально открывая автомобильный рынок для подготовленных и точных атак на отдельных лиц, конкурентов и политиков и т.п.

5) Национальные государства (Nation-states). Мотивы закамуфлированной деятельности представителей специальных служб национальных государств не всегда легко определить. Очевидными являются промышленный шпионаж, слежка, экономическая или реальная война. Другие мотивы связаны с вмешательством – «помощь» национальному производителю против иностранных конкурентов. Дополнительным фактором риска со стороны данной группы нарушителей является потенциальная возможность распространения сложного вредоносного кода, разработанного хорошо финансируемыми и специально подготовленными сотрудниками спецслужб национальных государств, в преступной среде, что существенно усиливает угрозу со стороны преступников и «шутников».

Анализ факторов риска и нарушителей позволяет строить модель угроз и модель нарушителя, которая предопределяет в дальнейшем обоснованность методов тестирования и корректность проведения испытаний элементов, устройств и систем интеллектуального транспортного средства.

В настоящее время нами определен следующий состав ключевых нормативных документов международного уровня, определяющих основные аспекты разработки и тестирования высокоавтоматизированных транспортных средств и интеллектуальных элементов дорожной инфраструктуры, включая сферу обеспечения кибербезопасности компонент интеллектуальной транспортной системы в целом:

– ISO/PAS 21448:2019 Road Vehicles – Safety of the intended functionality (SOTIF);
– ISO 26262:2018 Road Vehicles – Functional safety;
– ISO/SAE CD 21434 Road Vehicles – Cybersecurity engineering;
– ISO 19157:2013 Geographic information – Data quality;

– ISO/TS 19158:2012 Geographic information – Quality assurance of data supply;

– ISO/TS 16949:2009 Quality management systems – Particular requirements for the application of ISO 9001:2008 for automotive production and relevant service part organizations;

– ISO/IEC 2382-1:1993 Information technology – Vocabulary – Part 1: Fundamental terms;

– ISO/IEC/IEEE 15288:2015 Systems and software engineering – System life cycle processes.

Охарактеризуем 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, предложенные в работе [12]. Данное исследование было выполнено для решения проблем информационной безопасности технологий CAV при построении в Японии национальной ITS в рамках реализации проекта автоматического вождения для универсальных услуг (Automated Driving for Universal Services, ADUS) в составе Межведомственной программы содействия стратегическим инновациям (the Cross-ministerial Strategic Innovation Promotion Program, SIP). В рассматриваемой публикации понятие угроза была определена как «потенциальная ситуация (элемент), которая наносит вред (ущерб) автоматизированной системе вождения», что соответствует трактовке понятия угрозы в ISO / IEC 27000: 2009 [7] с уточнением, соответствующим цели исследования. На основе уточненного определения угрозы и введенных рабочей группой WP.29 положений Всемирного форума согласования правил в области транспортных средств[3] специалистами JSAE[4] были сопоставлены общая модель автоматизированной системы вождения и матрица угроз с целью выявления цели атаки и угрозы в отношении общей модели, которые затем были классифицированы на основе CAPEC[5].

Тип атаки и перечисление общих слабых мест (common weakness enumeration, CWE) использовались для сравнения и проверки результатов категоризации с точки зрения дефектов для создания списка угроз для общей модели автоматизированной системы вождения. В рамках проекта ADUS был выявлен следующий список угроз:

1) Угрозы, связанные с системой транспортного средства: утечка активов (информации) OEM-изготовителя, утечка личных данных владельца транспортного средства, утечка ключей шифрования, фальсифицированная программа управления транспортным средством, несанкционированное изменение идентификатора транспортного средства, подмена идентификатора транспортного средства, фальсификация данных вождения, несанкционированные данные диагностики транспортного средства, фальсификация/удаление данных журнала, фальсификация параметров функции контроля, фальсификация параметров функции оплаты, сбои в обслуживании из-за переполнения данных, внедрение вредоносных программ, обход систем мониторинга.

2) Угрозы, связанные с физическими внешними интерфейсами транспортного средства: подделка датчиков, фальсификация маршрутов передачи данных, заражение вирусом с внешних носителей, вторжение с физических внешних интерфейсов (USB и т.д.), отправка несанкционированного диагностического сообщения (OBD II и т.д.).

3) Угрозы, связанные с внутренними каналами связи транспортного средства: перехват связи, несанкционированный доступ к данным из канала связи, фальсификация данных связи, фальсификация функции связи (например, удаленных ключей), фальсификация данных связи ближнего действия / датчиков, непреднамеренное выполнение функции из-за внедрение команды, фаль-

[3] В рамках деятельности Отдела устойчивого транспорта Европейской экономической комиссии Организации Объединенных Наций (ЕЭК ООН).

[4] The Society of Automotive Engineers of Japan (JSAE) – Общество инженеров-автомобилестроителей Японии (см: https://www.jsae.or.jp/en/about/index.php).

[5] CAPEC - Common Attack Pattern Enumeration and Classification (A Community Resource for Identifying and Understanding Attacks). Информационный портал CAPEC предоставляет общедоступный каталог общих шаблонов атак, который помогает понять, как злоумышленники используют уязвимости в приложениях и другие кибер-поддерживаемых возможностях для угроз информационной безопасности. «Шаблоны атак» — это описания общих атрибутов и подходов, используемых злоумышленниками для использования известных недостатков в кибер-поддерживаемые возможностях. Шаблоны атак определяют проблемы, с которыми может столкнуться пользователь информационных систем, и способы их решения. Они вытекают из концепции шаблонов проектирования, применяемой в разрушительном, а не конструктивном контексте, и создаются на основе глубокого анализа конкретных примеров использования в реальных условиях.

сификация/перезапись/удаление/добавление данных/кода, заражение вирусом из каналов связи, отправка несанкционированных CAN-сообщений, отправка несанкционированных специальных сообщений (например, сообщения, разрешенные только для отправки от OEM-производителей), ввод данных из ненадежного источника, прерывание обслуживания из-за переполнения данных, подмены отправителя, гражданских атак, атак повторного воспроизведения.

4) Угрозы, связанные с внешними каналами связи транспортного средства: перехват канала связи, несанкционированный доступ к данным по каналам связи, атаки MITM, фальсификация/перезапись/удаление/добавление данных/кода, ввод данных из ненадежного источника, отправка несанкционированных сообщений V2X, заражение вирусом из канал связи, фальсифицированное стороннее приложение, нарушение обслуживания из-за переполнения данных, атака черной дыры в коммуникации V2V, гражданская атака, внедрение команд, атака воспроизведения, компрометация ядра программного обеспечения (bios) и учетной записи (root) владельца/оператора CAV и т.п.

5) Угрозы, связанные с внешним сервером: утечка информации из-за вторжения на сервер, утечки информации из-за несоответствующего обмена данными, захвата сервера из-за вторжения сервера, DoS-атаки на сервер, разрушения сервера из-за вторжений, несанкционированного использования CAV и объектов инфраструктуры.

6) Угрозы, связанные с сервисом обновлений: утечка ключа шифрования для обновлений, нарушение обновления/фальсификация программы обновления (серверная/локальная), внедрение несанкционированных данных обновления, нарушение авторизованного обновления.

7) Угрозы, связанные с атаками со стороны транспортного средства (вторичное повреждение): передача ненадежных данных V2V, атака по времени, отправка ложной экстренной информации, DoS-атаки с машины на другую систему, передача ненадежных данных в инфраструктуру, DoS-атаки против инфраструктуры, транспортного средства ботнета, DoS-атаки против сети.

8) Угрозы, связанные с физическими факторами: потеря данных из-за сбоя или другой аварии, потеря данных из-за сбоя в управлении DRM, потеря данных из-за сбоя в работе IT-компонента, утечка данных из-за перепродажи/покупки автомобиля владельцем, данные OEM фальсификации.

На основе аналитического подхода в исследовании [12] для 40 предполагаемых архитектур системы были определены из 35 уязвимых функций, которые используются 12 сервисами. Для каждой архитектуры системы было перечислено 72 угрозы, а категории WP.29, CWE и CAPEC были объединены для общей идентификации 3040 угроз. Из 579 угроз с вероятностью возникновения, которые были получены, с учетом архитектуры системы и применения Criticality Evaluation Framework идентифицировано 560 угроз, классифицированных как «Осторожно», 17 – «Предупреждение» и 2 – «Срочно». С помощью сформированной структуры оценок была рассчитана критичность угроз для каждой функции, которую включает система автоматизированного вождения. Из присущих угроз были извлечены угрозы с уровнем критичности уровня 2 или выше. Затем для 17 угроз, классифицированных как «Предупреждение», и двух угроз, классифицированных как «Срочно», были также определены контрмеры и ответственные стороны/субъекты для каждой контрмеры (контрмеры и ответственные были определены и включены в состав рекомендаций на основе руководящих принципов и общих требований для контрмер, рекомендованных в WP.29). Процедурные вопросы оценки угроз информационной безопасности были отражены в рекомендациях по оценке информационной безопасности отчета по проекту ADUS[6].

Таким образом, идентификация комплексной модели угроз для информационной безопасности ТП БА-ДИ может быть разработана на основе общей модели автоматизированной системы вождения при расширении зоны экспертной оценки до уровня интеллектуальных элементов ДИ и распределенной системы управления ITS (включая основные и резервные каналы коммуни-

[6] См.: http://www.sip-adus.go.jp/file/rd-result_all.pdf.

каций) с учетом структуры оценки критичности выявленных/ обозначенных угроз. Эта структура должна объединять различные критерии оценки, разработанные, например, в рекомендациях WP.29 для интегральной[7] оценки воздействия угрозы и степени атаки для измерения степени угрозы.

Для измерения эффектов негативных воздействий в ТП ВАТС-ДИ может быть использована следующая формула расчета степени критичности угрозы:

[влияние угрозы] × [степень разрушительности атаки] × [влияние инцидента] × [критичность информационного актива] = критичность угрозы.

Все возможные угрозы при анализе построения ITS и ТП ВАТС-ДИ в ходе исследования должны выявляться с учетом архитектуры систем и устройств транспортного средства, связанных с автоматизированной системой вождения и подключенных тем или иным образом к единому информационному полю, которое поддерживается общей сетью доступа (V2X).

Идентификация и дифференциация угроз, на которые нужно ответить с тем или иным приоритетом, могут определяться с использованием эвристической системы оценки критичности. Для специфицированного спектра угроз должны быть определены ответственные лица за состояние информационной безопасности компонент ITS и контрмеры по противодействию угрозам, а также требования к верификации и валидации системы автоматизированного вождения при тестировании технологий CAV и сертификации CAV (и отдельных компонент ТП ВАТС-ДИ). Все необходимые контрмеры (на стороне аппаратно-программных комплексов как инфраструктуры ITS, так и транспортного средства) должны были отражены в технологическом стандарте разработки и эксплуатации беспилотного транспорта и соответствующих руководствах по оценке и обеспечению информационной безопасности ITS и CAV.

Общая модель автоматизированной системы вождения для исследования угроз интеллектуальному транспортному средству в рамках использования платформы V2X изображена на рис. 3.

Направления дальнейших исследований

Рассмотренные подходы к идентификации и анализу зон уязвимости информационной безопасности беспилотных автомобилей и состава угроз информационного взаимодействия подключенных и автономных транспортных средств с активными элементами дорожной инфраструктуры позволяют охарактеризовать сложность и масштабность задач создания национальной интеллектуальной транспортной системы. Дальнейшие исследования в области обеспечения информационной безопасности технологической платформы Vehicle-to-Everything (V2X) связаны с разработкой методики тестирования беспилотных автомобилей различного назначения, а также с формированием комплекса национальных стандартов для ITS, сопряженных с обобщением национальных и международных требований обеспечения интероперабельности и мультимодальности устройств и технологий CAV для «бесшовного» построения глобальных транспортных коридоров. Кроме того, необходима разработка унифицированных технических и организационных требований к проектам испытательных стендов (реальное и виртуальное лабораторное тестирование) и испытательных полигонов (ситуационная и комплексная дорожная эксплуатация) для беспилотного транспорта и его отдельных компонентов. Весь комплекс вопросов создания/ внедрения технологий CAV и построения/ функционирования ITS должен быть также адекватно отражен при обосновании и адаптации нормативных правовых актов в национальном законодательстве. Отдельного внимания заслуживает решение исследовательских задач в области моделирования трансформации дорожной сети и транспортных потоков, а также экономического анализа динамической модели жизненного цикла как отдельного беспилотного автомобиля конкретного типа и назначения, так и ITS в целом.

[7] В указанной публикации отсутствуют подробности описания расчетов, но анализ формы представления результатов позволяет сделать вывод, что, по существу, использовалась порядковая шкала идентификации значений по различным аспектам экспертной оценки угроз.

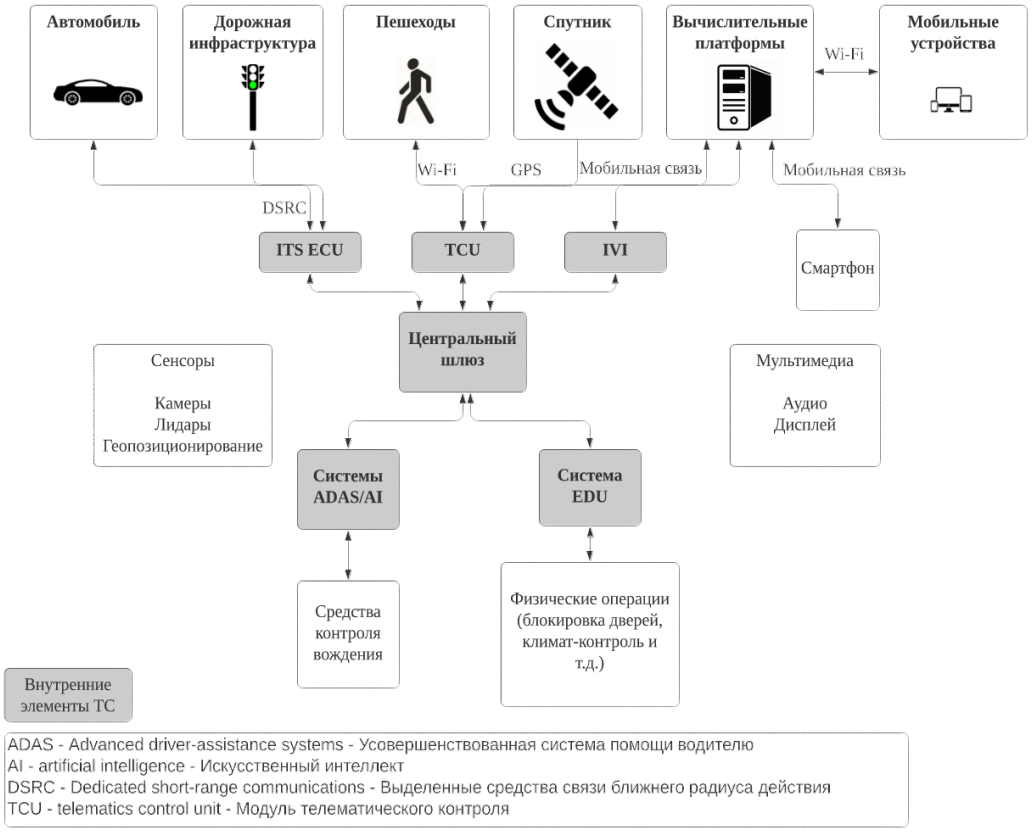

Рис. 3. Общая модель автоматизированной системы вождения
для выявления и анализа угроз взаимодействию транспортного средства с инфраструктурой ITS
Источник: адаптировано авторами на основе SIP Program Directorate (project ADUS)[8]

Fig. 3. A general structural model of an automated driving system for identifying and analyzing threats
to the interaction of an unmanned vehicle with ITS infrastructure

Заключение

К настоящему времени общей тенденцией использования достижений науки и техники в области цифровой трансформации использования транспортных средствах стало расширение спектра автоматизированных функций или систем. Первоначально основной задачей здесь выступало обеспечение безопасности вождения транспортного средства через облегчение функций управления с целью сделать управление автомобилем максимально легким, а поездку более комфортной. Для решения этой задачи расширялись функции электронных систем автомобиля и датчиков, при этом оценка ситуации, принятие решений и управление оставались за водителем. Однако дальнейшее развитие таких систем не ведут к существенному снижению безопасности. Поэтому последующие шаги по автоматизации вождения ориентированы на анализ обстановки, принятие решений и управление автомобильным комплексом, в который включен как высокоавтоматизированный автомобиль (BATC, CAV), так и дорожная инфраструктура, а также глобальные сервисы. Подобная система не только обеспечивает повышение безопасности движения, но и позволяет использовать информацию об окружающей обстановке для снижения совокупных затрат системы за счет оптимизации маршрута движения, контроля расхода топлива, уменьшения негативного воздействия на окружающую среду и др. [13–15].

Вместе с тем, очевидно, что автоматизированное и тем более автоматическое управление транспортным средством представляет собой очень сложную задачу, в этой связи замена води-

[8] См.: http://www.sip-adus.go.jp/file/rd-result_all.pdf

теля-человека компьютером является реальной проблемой с технической, организационной и правовой стороны [16–18]. Общий уровень безопасности транспортных систем потенциально может снижаться из-за наличия электронных компонентов, возросшей сложности бортовой системы автоматизированного вождения, широкого применения автоматизированного регулирования автомобильного движения, а также интенсивных цифровых коммуникаций транспортного средства с внешним дорожным окружением. С одной стороны, технологии машинного зрения и искусственного интеллекта позволяют уменьшить риски дорожных инцидентов с участием CAV. С другой стороны – расширяется спектр угроз, связанных с возможным нарушением функциональной целостности и работоспособности CAV вследствие преднамеренных воздействий на компоненты системы автоматизированного вождения транспортного средства, каналы информационного взаимодействия с дорожной инфраструктурой, включая центры управления движением в рамках ITS.

Таким образом, сложившаяся ситуация требует дальнейшего совершенствования норм и требований правового и технического регулирования создания и эксплуатации CAV различного назначения на участках дорог локального и общего пользования, что предполагает расширение области и задач тестирования безопасности автомобильного общественного, личного, коммерческого и специального транспорта, в том числе за счет проверки информационной безопасности при валидации и верификации как CAV, так и компонентов ITS [19–22]. В этой связи с позиций обеспечения национальной безопасности в области развития беспилотного транспорта для различных сред (наземного, воздушного и водного) ключевое значение для Российской Федерации в настоящее время приобретает задача формализации научных достижений и практического опыта по разработке надежных беспилотных технологий для построения эффективной национальной системы стандартизации и сертификации в области CAV и ITS с целью обеспечения безопасности технологической платформы информационного взаимодействия высокоавтоматизированного транспорта с окружающей дорожной инфраструктурой, что позволит повысить в цифровой среде уровень безопасного автоматизированного (подключенного и автономного) автомобильного движения.

В ходе проведенного исследования проблем обеспечения информационной безопасности беспилотных технологий были получены научные результаты в части определения зон уязвимостей CAV во взаимосвязи с характеристиками спектра угроз и состава акторов несанкционированного нарушения штатного функционирования платформы V2X для информационных взаимодействий в рамках ITS.

На основе представленной модели угроз информационной безопасности CAV могут быть разработаны методические подходы и аналитические инструменты для организации и тестирования в рамках лабораторных экспериментов и полигонных испытаний различных видов преднамеренных нарушений каналов информационного взаимодействия отдельных устройств CAV, группы автономных транспортных средств и отдельного CAV с ITS. После закрепления нормативных требований в отечественном стандарте информационной безопасности CAV возможными направлениями дальнейших исследований могут стать: разработка методических рекомендаций для оценки риска информационной безопасности CAV на основе экономического анализа последствий инцидентов в среде ITS для набора вероятностных и стоимостных характеристик рисковых событий с беспилотными автомобилями личного, общественного, коммерческого и специального назначения; разработка технологической и экономической моделей тестирования информационной безопасности в рамках ITS для национальной системы сертификации CAV различного типа.

Благодарности

Статья подготовлена в рамках исследования по теме № 7269-19 «Разработка концепции создания полигона для отработки технологий взаимодействия «беспилотный автомобиль – дорож-

ная инфраструктура» с учетом угроз безопасности для интеллектуальных транспортных систем и беспилотных автомобилей», выполненной по заданию ФАУ «Российский дорожный научно-исследовательский институт» в интересах Минтранса России.

СПИСОК ЛИТЕРАТУРЫ

1. Autonomous Driving. Technical, Legal and Social Aspects / Eds. M. Maurer, J. Gerdes, B. Lenz, H. Winner. Berlin: Springer, 2016. – 706 p. DOI: 10.1007/978-3-662-48847-8)

2. The C-ITS Platform: Phase I. Final report of January 2016. Электронный ресурс URL: https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf (дата обращения: 12.07.2020).

3. **Li L., Huang W., Liu Y., Zheng N., Wang F.** Intelligence Testing for Autonomous Vehicles: A New Approach, IEEE Transactions on Intelligent Vehicles. IEEE Transactions on Intelligent Vehicles. 2016: 1(2), pp. 158–166. DOI: 10.1109/TIV.2016.2608003/

4. Perspectives on the Use of New Information and Communication Technology (ICT) in the Modern Economy. Springer International Publishing AG, 2019, 1178 p. DOI: https://doi.org/10.1007/978-3-319-90835-9

5. **Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H., Savage S., Koscher K., Czeskis A., Roesner F., Kohno T.** Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association. Berkeley, USA, 2011. 6 p.

6. **Rosenquist M.** Prioritizing Information Security Risks with Threat Agent Risk Assessment. Intel Corp. 2009. Электронный ресурс URL: https://communities.intel.com/servlet/JiveServlet/download/4693-1-3205/Prioritizing_Info_Security_Risks_with_TARA.pdf (дата обращения: 12.07.2020).

7. ISO / IEC 27000: 2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary. Электронный ресурс URL: https://www.iso.org/standard/41933.html (дата обращения: 12.07.2020).

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

9. **Komarov T., Ivanov M., Chepik N., Starikovskiy A.** Development of fast and memory-safe operating system kernel: Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2019, 2019, pp. 1852–1856.

10. **Ivanov M.A., Roslyj E.B., Starikovskiy A.V., Krasnikova S.A., Shevchenko N.A., Shustova L.I.** Non-binary pseudorandom number generators for information security purposes: Procedia Computer Science, 2018г. T. 123, Q2, pp. 203-211. 8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017.

11. White paper. Automotive Security: Best Practices. Recommendations for security and privacy in the era of the next-generation car / McAfee. Santa Clara, USA: McAfee, 2016. – 21 p.

12. **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. In SIP-adus: Project Reports, 2014-2018 – Automated Driving for Universal Services. Publisher's Office Cabinet Office, Government of Japan, 2019, pp. 77–83.

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

14. Automated Vehicles Index: 1Q, 2016. Munich: Publisher Roland Berger GmbH, 2015. 18 p.

15. **Anderson J., Kalra N., Stanley K., Sorensen P., Samaras C., Oluwatola O.** Autonomous Vehicle Technology: A Guide for Policymakers / Rand Corporation. Santa Monica, USA, 2016. – 214 p.

16. **Степанян А.Ж.** Проблемы регулирования беспилотных транспортных средств // Вестник Университета имени О.Е. Кутафина, 2019. № 4(56). С. 169–174.

17. The Economic and Social Value of Autonomous Vehicles. Compass Transportation and Technology, Inc. – Stackhouse, USA, 2018. 58 p.

18. Digital Security in a Networked World. Hoboken, USA: Wiley, 2015. – 448 p.

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

20. **Писарева О.М., Алексеев В.А., Медников В.А., 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.

21. **Pisareva O.M., Alexeev V.A., Mednikov D.N., Starikovsky A.V., Kurguzov V.B.** Creating a national certification system for unmanned vehicles: tasks of information security testing. St. Petersburg State Polytechnical University Journal. Economics. 2021. Vol. 14. No 2. P. 63–80.

22. **Taeihagh A., Lim H.S.M.** Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transport Revue. 2019, # 39(1), P. 103–128.

23. **Yaacoub J.-P., Noura H., Salman O., Chehab A.** Security analysis of drones systems: Attacks, limitations, and recommendations // Internet of Things, Vol. 11, September 2020, 100218. Электронный ресурс URL: https://www.sciencedirect.com/science/article/abs/pii/S2542660519302112?via%3Dihub (дата обращения: 27.07.2021).

24. **Zou B., Choobchian P., Rozenberg J.** Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies // Journal of Transportation Security, 2021. Электронный ресурс URL: https://link.springer.com/article/10.1007/s12198-021-00230-w (дата обращения: 27.07.2021).

REFERENCES

1. Autonomous Driving. Technical, Legal and Social Aspects / Eds. M. Maurer, J. Gerdes, B. Lenz, H. Winner. Berlin: Springer, 2016. – 706 p. DOI: 10.1007/978-3-662-48847-8)

2. The C-ITS Platform: Phase I. Final report of January 2016. Elektronnyy resurs URL: https://ec.europa.eu/transport/sites/transport/files/themes/its/doc/c-its-platform-final-report-january-2016.pdf (data obrashcheniya: 12.07.2021).

3. **L. Li, W. Huang, Y. Liu, N. Zheng, F. Wang,** Intelligence Testing for Autonomous Vehicles: A New Approach, IEEE Transactions on Intelligent Vehicles. IEEE Transactions on Intelligent Vehicles. 2016: 1(2), pp. 158–166. DOI: 10.1109/TIV.2016.2608003/

4. Perspectives on the Use of New Information and Communication Technology (ICT) in the Modern Economy. Springer International Publishing AG, 2019, 1178 p. DOI: https://doi.org/10.1007/978-3-319-90835-9

5. **S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno,** Comprehensive experimental analyses of automotive attack surfaces. In Proceedings of the 20th USENIX conference on Security (SEC'11). USENIX Association. Berkeley, USA, 2011. 6 p.

6. **M. Rosenquist,** Prioritizing Information Security Risks with Threat Agent Risk Assessment. Intel Corp. 2009. Elektronnyy resurs URL: https://communities.intel.com/servlet/JiveServlet/download/4693-1-3205/Prioritizing_Info_Security_Risks_with_TARA.pdf (data obrashcheniya: 12.07.2020).

7. ISO / IEC 27000: 2009 Information technology – Security techniques – Information security management systems – Overview and vocabulary. Elektronnyy resurs URL: https://www.iso.org/standard/41933.html (data obrashcheniya: 12.07.2021).

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

9. T. Komarov, M. Ivanov, N. Chepik, A. Starikovskiy, Development of fast and memory-safe operating system kernel: Proceedings of the 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, ElConRus 2019, 2019, pp. 1852–1856.

10. **M.A. Ivanov, E.B. Roslyj, A.V. Starikovskiy, S.A. Krasnikova, N.A. Shevchenko, L.I.Shustova,** Non-binary pseudorandom number generators for information security purposes: Procedia Computer Science, 2018g. T. 123, Q2, pp. 203–211. 8th Annual International Conference on Biologically Inspired Cognitive Architectures, BICA 2017.

11. White paper. Automotive Security: Best Practices. Recommendations for security and privacy in the era of the next-generation car / McAfee. Santa Clara, USA: McAfee, 2016. – 21 p.

12. **K. Okuyama,** 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. In SIP-adus: Project Reports, 2014-2018 – Automated Driving for Universal Services. Publisher's Office Cabinet Office, Government of Japan, 2019, pp. 77–83.

13. **A.G. Nosov,** Ekonomicheskiye i infrastrukturnyye aspekty razvitiya tekhnologiy bespilotnogo transporta // Transport Rossiyskoy Federatsii, 2016. № 5. S. 21–25.

14. Automated Vehicles Index: 1Q, 2016. Munich: Publisher Roland Berger GmbH, 2015. 18 p.

15. **J. Anderson, N. Kalra, K. Stanley, P. Sorensen, C. Samaras, O. Oluwatola,** Autonomous Vehicle Technology: A Guide for Policymakers / Rand Corporation. Santa Monica, USA, 2016. – 214 p.

16. **A.Zh. Stepanyan,** Problemy regulirovaniya bespilotnykh transportnykh sredstv // Vestnik Universiteta imeni O.Ye. Kutafina, 2019. № 4(56). S. 169–174.

17. The Economic and Social Value of Autonomous Vehicles. Compass Transportation and Technology, Inc. – Stackhouse, USA, 2018. 58 p.

18. Digital Security in a Networked World. Hoboken, USA: Wiley, 2015. – 448 p.

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

20. **O.M. Pisareva, V.A. Alekseyev, V.A. Mednikov, A.V. Starikovskiy,** Razvitiye intellektualnykh transportnykh sistem v Rossiyskoy Federatsii: opredeleniye trebovaniy i organizatsiya sozdaniya poligonov testirovaniya informatsionnoy bezopasnosti // Nauchno-tekhnicheskiye vedomosti SPbGPU. Ekonomicheskiye nauki. 2020. T. 13, № 5. S. 7–23.

21. **O.M. Pisareva, V.A. Alexeev, D.N. Mednikov, A.V. Starikovsky, V.B. Kurguzov,** Creating a national certification system for unmanned vehicles: tasks of information security testing. St. Petersburg State Polytechnical University Journal. Economics. 2021. Vol. 14. No. 2. P. 63–80.

22. **A. Taeihagh, H.S.M. Lim,** Governing autonomous vehicles: emerging responses for safety, liability, privacy, cybersecurity, and industry risks. Transport Revue. 2019, # 39(1), P. 103–128.

23. **J.-P. Yaacoub, H. Noura, O. Salman, A. Chehab,** Security analysis of drones systems: Attacks, limitations, and recommendations // Internet of Things, Volume 11, September 2020, 100218. Электронный ресурс URL: https://www.sciencedirect.com/science/article/abs/pii/S2542660519302112?via%3Dihub (дата обращения: 27.07.2021).

24. **B. Zou, P. Choobchian, J. Rozenberg,** Cyber resilience of autonomous mobility systems: cyber-attacks and resilience-enhancing strategies // Journal of Transportation Security, 2021. Электронный ресурс URL: https://link.springer.com/article/10.1007/s12198-021-00230-w (дата обращения: 27.07.2021).

Статья поступила в редакцию 29.06.2021.

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: avstarikovskiy@gmail.com
STARIKOVSKIY Andrew V.
E-mail: avstarikovskiy@gmail.com