DOI: 10.18721/JE.14204
UDC 338.47 : 330.47 : 656.13 : 004.056

CREATING A NATIONAL CERTIFICATION SYSTEM FOR UNMANNED VEHICLES: TASKS OF INFORMATION SECURITY TESTING

O.M. Pisareva[1], V.A. Alexeev[3], D.N. Mednikov[1], A.V. Starikovsky[1], V.B. Kurguzov[2]

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

[2] ROSDORNII FAU, Moscow, Russian Federation;

[3] Rabus LLC, Moscow, Russian Federation

Currently, digital technologies are penetrating all spheres of public life and are rapidly changing the economic landscape of each country. The transport industry is actively introducing technical and organizational solutions related to the creation of self-driving cars and their safe operation. The transition to the widespread introduction of unmanned vehicles is associated not only with new opportunities for personal mobility and commercial logistics, but also with the emergence of new risks of using artificial intelligence technologies in vehicle traffic control and traffic regulation systems. In this regard this study is devoted to the creation of a procedure and mechanism for state certification of unmanned vehicles. The relevance of the study is determined by the characteristics of innovative solutions in this problem area and the high social value of ensuring transport security, including the protection of information interactions within the framework of intelligent transport systems. In the course of the study, the authors have given a definition of certification of information security of vehicles. The article discusses domestic and foreign experience in building certification systems for complex technical systems, including the assessment of means and mechanisms to ensure their safe operation. An analysis of the content and process of certification of unmanned vehicles was carried out from the standpoint of verifying compliance with information security requirements. The object, subject and goals of certification of unmanned vehicles are formulated. The work defines the composition and specificity of the tasks solved in the course of certification. The characteristics of the methods and procedure for certification of unmanned vehicles are given. The structure, regulations and mechanism for certification of unmanned vehicles have been determined. Based on the results of the study, the authors substantiated recommendations for improving the institutional framework and developing organizational solutions for creating a national certification system for unmanned vehicles. It also provides a characteristic of promising research tasks in the development of methodological support for the design of test platforms. The authors proposed a set of measures for creating planning tools and conducting tests to assess compliance with information security requirements for unmanned vehicles.

Keywords: unmanned vehicles, digital technologies, information security, threat modeling, testing profile, software certification, hardware certification, activity's licensing, state accreditation, economic model of certification

Citation: 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, 14 (2) (2021) 63–80. DOI: 10.18721/JE.14204

ПОСТРОЕНИЕ НАЦИОНАЛЬНОЙ СИСТЕМЫ СЕРТИФИКАЦИИ БЕСПИЛОТНОГО АВТОТРАНСПОРТА: ЗАДАЧИ ТЕСТИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Писарева О.М.[1], Алексеев В.А.[3], Медников Д.Н.[1], Стариковский А.В.[1], Кургузов В.Б.[2]

[1] Государственный университет управления, Москва, Российская Федерация;

[2] ФАУ «РОСДОРНИИ», Москва, Российская Федерация;

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

Цифровые технологии проникают во все сферы общественной жизни и стремительно меняют экономический ландшафт каждой страны. В транспортной отрасли активно создаются технические и организационные решения, связанные с созданием беспилотных транспортных средств и их безопасной эксплуатацией. Переход к широкому внедрению беспилотных автомобилей связан не только с новыми возможностями персональной мобильности и коммерческой логистики, но также и с возникновением новых рисков использования технологий искусственного интеллекта в системах управления движением автомобиля и регулирования транспортных потоков. В связи с этим настоящее исследование посвящено вопросам создания порядка и механизма государственной сертификации беспилотных автомобилей. Актуальность исследования определяется характеристикой инновационности решений в данной проблемной области и высоким социальным значением обеспечения транспортной безопасности, включая защиту информационных взаимодействий по различным каналам связи в рамках интеллектуальных транспортных систем. В ходе исследования авторами было дано определение сертификации информационной безопасности транспортного средств. В работе рассмотрен отечественный и зарубежный опыт построения систем сертификации сложных технических систем, включая оценку средств и механизмов обеспечения их безопасной эксплуатации. Был выполнен анализ содержания и процесса сертификации беспилотных автомобилей с позиций проверки обеспечения требований информационной безопасности. Сформулированы объект, предмет и цели сертификации беспилотных автомобилей. В работе определены состав и специфика решаемых в ходе сертификации задач. Дана характеристика методов и порядка сертификации беспилотных автомобилей. Определены структура, регламент и механизм сертификации беспилотных автомобилей. На основе результатов исследования авторами были обоснованы рекомендации по совершенствованию институциональной основы и разработке организационных решений для создания национальной системы сертификации беспилотных автомобилей. Также дана характеристика перспективных исследовательских задач в области разработки методического обеспечения проектирования тестовых платформ. Авторами предложен состав мер для создания инструментария планирования и проведения тестовых испытаний по оценке соблюдения требований информационной безопасности беспилотного автотранспорта.

Ключевые слова: беспилотный транспорт, цифровые технологии, информационная безопасность, моделирование угроз, профиль тестирования, сертификация программного обеспечения, сертификация технических средств, лицензирование, аккредитация, экономическая модель сертификации

Ссылка при цитировании: Писарева О.М., Алексеев В.А., Медников Д.Н., Стариковский А.В., Кургузов В.Б. Построение национальной системы сертификации беспилотного автотранспорта: задачи тестирования информационной безопасности // Научно-технические ведомости СПбГПУ. Экономические науки. 2021. Т. 14, № 2. С. 63–80. DOI: 10.18721/JE.14204

Introduction

Implementation of technological innovation projects becomes pivotal for creating necessary conditions for strategic tasks of the Russian Federation and achieving socio-economic development goals. This technological innovation will contour outlines of the national economic complex of the country. Transportation is one of the areas for perspective technical solutions deployment. Introduction of digital technologies leads to deep transformations of traffic management systems, and, as it is often the case with innovations, is associated with the emergence of new risks for unmanned vehicles safety.

The object of the present research is the transportation system of the Russian Federation. The subject of the research is developing a framework for information security service certification which is used for smart digital traffic management. The main goal of the study is to determine the key principles and tasks of creating a national certification system for unmanned vehicles. These tasks are linked to the technical solutions and organizational aspects for the development of testing grounds for information security level of tech platforms integrating an unmanned vehicle and road infrastructure. The tech platforms are created and introduced to the market of transportation services.

Caused by the general issue of ensuring road safety and the reasoning of state regulation of the technological development of the transport system, the main tasks of the study are to analyze existing approaches to ensuring the security of information interaction of connected and autonomous vehicles with active components of an intelligent transport system infrastructure (the so-called technological platform: Vehicle-to-Everything or V2X); to assess the impact of unmanned vehicle technologies on the socio-economic development of the country and determine the content and specifics of certification of unmanned vehicles from the standpoint of verifying information security requirements; to define the object, subject and purposes of unmanned vehicles certification; to typify the tasks, methods and procedures for certification of unmanned vehicles; to define structure, regulations and mechanism of the certification procedure for unmanned vehicles; to develop recommendations for improving the institutional framework and management procedures as a basis of establishing a national certification system for unmanned vehicles and the V2X technology platform used for building an intelligent transport system on a city, regional and national scale.

Vision of the future transport system with digital technologies employed

The creation of unmanned vehicles for land, air and water transport is one of the leading trends in scientific and technological development, which largely determines the future shape of the knowledge-based economy [1]. The development of unmanned vehicles (UVs) for various purposes is of great economic and social importance as a field of innovations that combine a number of advanced scientific approaches and technical solutions (from the so-called key end-to-end technologies of the new industrial wave: big data, artificial intelligence, wireless communication, internet of things, etc.). The functions of driver support (drive assist), partial automation and conditional automation when driving personal and commercial vehicles have become standard for 1, 2 and 3 classes of UV as per the SAE International classification system that is generally accepted in the professional environment. Experts state the further expansion of digital technologies to support production and organizational processes of road transportation in urban, intercity and main road traffic, assessing the transition from the emerging 4 UV class (limited automation) to the 5 UV class (full automation) after 2025 (https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety).

The transportation industry is of key importance for the integration of the entire economic complex of the Russian Federation spatial structure due to its vast territories. It shapes the opportunities for establishing convenient international transport corridors with multimodal transportation as well [2]. While it is too early to talk about a full-fledged market of autonomous vehicles (only some regions allowed limited operation of prototypes of UVs within certain sections of public-access roads), it is important to prevent the growth of the relative lag of the Russian Federation in the field of developing in-

telligent transport systems (ITS) and developing hardware and software complexes for automatic driving systems (IDS)[1]. Today the basics are being laid to establish the mechanisms for the distribution of a kind of technological rent in the field of passenger traffic and cargo traffic, that are optimized at the national and international levels of the economy, taking into account the evolution of the technical base of the transport industry and the restructuring of demand for transport services.

Catching up development: from import substitution to technological leadership

The transformation of the geopolitical and geoeconomic systems has caused appearance of the mechanism of unilateral restrictions in international relations as a tool of unfair competition to restrain economic and technological development in the segmented world of the renewed project of globalization. This leads to establishing of a "safety net" in the system of global affairs and cooperation[2] in various fields to minimize the risks of successful implementation of national projects in the internal agenda of dynamic and sustainable socio-economic development (SED) of the Russian Federation.

Therefore, the issues of deploying highly automated vehicles in the Russian Federation, including unmanned vehicles, should be the focus of the state's attention. It will contribute to the safe use of imported and localized technical devices (and corresponding technological protocols, standards and regulations) for intelligent transport systems. Moreover, it would be also beneficial to the establishing of sustainable demand for domestic analogues of hardware components[3] for computer and communication equipment which is crucial for critical information infrastructure facilities [3]. In the latter case, the obvious consequence will be the active recovery of domestic microelectronics by means of employing the strengths of the Russian science and engineering schools in the development of analytical, algorithmic methodology and software for the core of an automatic vehicle control system and a traffic control system with the participation of autonomous and connected vehicles.

In modern conditions, the implementation of technical and organizational innovations portfolio is linked with the emergence of new aspects of ensuring national security in the development and application of digital technologies. A significant part of it is associated with the use of foreign solutions and components for information-communication systems and hardware-software complexes for various purposes. In this regard, Russian science and business should be focused on and stimulated to develop original technologies and establish their own production of the entire range of components for UV and ITS, taking into account the advanced experience of foreign manufacturers. It is noteworthy that in the case of analysis of imported software and devices (components and finished products), we are talking about the aspects of assessing compliance with national requirements and regulations of products and technologies already prepared for practical use with a preliminary assessment of their economic efficiency and commercial potential. In this case, the strategy consists in leading domestic developers towards the implementation of the catch-up development opportunities. Firstly, they ensure the total costs reduction within the life cycle of tested products and technologies. And secondly, they provide concentration of resources on innovative projects in certain areas with a relative competitive advantage of the

[1] In ITS smart roads ecosystem includes solutions for collecting and processing data on vehicles and road infrastructure for decision-making by road users, including operators of connected and autonomous vehicles: adaptive (smart) traffic lights; means of automatic recording of violations of traffic rules (SDA); monitoring systems for difficult road sections; electronic means of non-stop fare payment; electronic means of payment for parking (parking meters); connected information boards; traffic flow detectors; automatic weight and dimensional control systems; automated lighting control systems; GPS / GLONASS positioning systems; other connected objects, for example, automatic road weather stations, road controllers, travel stops (barriers), etc.

[2] The well-known concept was reformulated in a statement by the Minister of Foreign Affairs of the Russian Federation S.V. Lavrov, who commented on September 13, 2020, in the information and analytical program of the All-Russian State Television and Radio Broadcasting Company (VGRTK), the situation with the EU's actual refusal to implement its own strategic interests in the development of mutually beneficial economic integration (see: https://www.vesti.ru/article/2457436).

[3] New technical solutions for the national ITS ecosystem should be created in accordance with the requirements of the Federal Law "On the Security of the Critical Information Infrastructure of the Russian Federation" dated July 26, 2017 No. 187-FZ and the order of the Government of the Russian Federation dated January 17, 2020 No. 20-r "On the Strategy for the Development of the Electronic Industry of the Russian Federation for the Period up to 2030 and the Action Plan for its Implementation". In particular, the roadmap currently being developed for the project "New Generations of Microelectronics and the Creation of an Electronic Component Base" provides for financing of work in the amount of 798 billion rubles until 2024 (see: https://www.cnews.ru/news/top/2020-09-07_rossijskaya_mikroelektronika).

national scientific and engineering schools. The design, production and operation of the UV requires a thorough analysis and comprehensive accounting for emerging risks in the field of ensuring the safety of transport communications. When creating control systems for a vehicle and developing intelligent complexes for traffic regulation, the safety of road traffic in the context of an expanding range of digital technologies used is linked, first of all, with ensuring the protection of information interaction of the UV with the road infrastructure (RI), i.e. cybersecurity of the V2X (Vehicle-to-Everything) technological platform within the ITS [4].

Thus, along with direct state support for research and technical development in the field of autonomous vehicles, it is important to use institutional and organizational measures to regulate the emerging technology sector for highly automated vehicles, including proactive arrangements of conditions for the efficiency and competitiveness of technical solutions for autonomous vehicles in future national transport system vision. In the context of the international competition in the field of high-tech, the dominant country (countries) use protectionist measures to protect their leadership[4]. Under such circumstances, the lagging state, along with legal, but not very effective for ensuring national interests, retaliatory sanctions actions, which are caused by external illegal unilateral restrictions, has a completely legal and rather effective instrument for regulating the sphere of technological cooperation for the purpose of sustainable SED: the Institute for Certification of Products and Services. It is important that its application is carried out from the standpoint of ensuring the safety of using ITS components and technologies for the life and health of consumers.

Certification as a tool to support technological development

Certification, which emerged as a protection tool, has evolved into a complex toolkit, which has especially fully revealed its functionality in the digital environment of network forms of agent relationships in the field of end-user protection, the economic partnerships establishing, as well as the support and regulation of national technical / technological development [5, 6, 7, 8, etc.]. Certification as a state control tool is a legitimate way to reduce the exclusive offer of imported goods and increase the export potential of the goods of similar / interchangeable categories. The institute of certification solves the issue of ensuring the price and non-price competitiveness of the domestic industry in the state internal and foreign markets for high-tech complex products: requirements and restrictions simultaneously play the role of technological and antimonopoly regulation. The certification allows the use of state control on functional properties, quality characteristics and safety of products and technologies as a basis for: evaluation of the modern scientific and technical level; assessment of the sensitivity of the requirements of national standards and technological regulations; identification of the prospects for the localization of production; correction of the national research and development program.

Safety requirements for products / services are a universal way of organizing and implementing the homologation[5] of imported equipment (and technologies, if we consider the procurement of industrial equipment) of the UVs for the purpose of the following localization of the production of components / products. This creates the basis for the further restoration and establishing necessary engineering-technical and production-technological competencies centers with developing corresponding industry clusters in the national economy. Thus, certification of products / services will indirectly contribute to over-

[4] Of course, now this leadership of the so-called developed countries of the outgoing technological generation is de facto extremely unstable, taking into account both the growth rates of new world centers of economic power and scientific and technical competencies, and the specific properties of common knowledge as a commodity in the networked global economy. However, this instability is also the reason the developed countries are taking comprehensive measures to carefully protect their leadership positions in accordance with the commercial interests of transnational corporations, which have a highly concentrated and well-functioning legal and organizational mechanism for controlling industrial assets and financial flows.

[5] Homologation – bringing the technical characteristics of a product in line with the standards of the importing country in the certification process [9, 10, 11, etc.]. This general term defines the scope of tasks and the content of the process of determining the degree of suitability of communication equipment and assessing its compliance with national requirements (regional / local, if we are talking about operation in territories with special modes of economic activity, including nature reserves). The necessary checks usually consist in comprehensive testing, including checking the technical condition diagnostic systems, analyzing the signaling systems for operating modes and malfunctions, evaluating various aspects of operational safety, characterizing electromagnetic compatibility, etc.

coming the negative consequences of the process of restrictions on equal cooperation and on exports associated with the revival of "bloc thinking" in the "developed" countries and the use of tools of competition in the spheres of economic development and political containment of "unwanted" countries, especially in the framework of the trade turnover of components, equipment and double-purpose technologies, which are widely represented in the control complexes of UV. Of course, first of all, in order to overcome strategic gaps and technological backwardness, it is necessary to support national projects of scientific research and technical development (including joint ones), but it is equally important to create legal foundations and organizational mechanisms for ensuring scientific and technological development. The institute for certification of products and services (more broadly, technological platforms) can play a special role here. Obviously, as for controlled penetration of foreign products and technologies, and for the development of own research and production base for the effective use of the certification institute in regulating the domestic UVs market, it is important to timely design and correct the content of national technological standards and regulations. At the same time, a kind of general mechanism of coercion to innovations is being developed: state measures to accelerate and regulate technological development corridors are associated with financing the establishment of uniform regulatory requirements and standard technical solutions. It is also true for the ITS sphere, where integration is possible only on the basis of a common digital platform (the principle of interoperability and scalability in the escalation of relevant investment projects at the international, national, federal, regional and municipal levels).

Thus, in the field of development and application of digital UV technologies, it is required to implement a set of state measures to support technological and organizational innovations, including the development of a regulatory framework and technical solutions, an organizational mechanism and an economic model for a certification system in the market for testing devices and technologies to provide a cybersecurity technological platform (TP) of the interaction of the UV with the DI when establishing the rules and procedures for the accreditation of operators of the following services.

Object, subject and purposes of certification

Under the expansion of digital technologies and the increasingly complex electronic communications environment, cybersecurity is the most dynamically developing and critically important area for the global connectivity of all spheres of society, including economic activity in an unmanned environment. The security of autonomous and connected vehicles allowed to special and public roads must be properly established for the range of possible information threats of the regular operation of automatic driving systems and interaction with active and passive components of the road infrastructure. Certification (from lat. "Certum" – right, "facere" – to do) is a procedure carried out by the authorized body to confirm the compliance of the inspected objects with the established requirements of technical regulations and the provisions of national standards in the form of issuing a following certificate (in order to certify operational safety and application characteristics). The certification mode can be voluntary (professional certification) and mandatory (state certification). TP UV-DI cybersecurity certification based on the results of testing (analysis, assessment, validation, verification) refers to the sensitive area of ensuring personal and public data and safety, therefore, it should be mandatory for all ITS equipment market participants, UV for various purposes and transport services provided on the basis of UV.

Regarding the ITS, the object of UV cybersecurity certification is a wheeled vehicle[6] with installed electronic equipment and software for automation systems for driving a car in a traffic stream and systems for information interaction with other road users and elements of road infrastructure. During the audit, the subject of certification is to identify the individual characteristics of the cybersecurity of the evaluated UV, analyze how these characteristics match with the declared parameters of the UV developer / manufacturer, and determine the degree of stability of the UV cybersecurity maintenance system in

[6] An alternative wording is electronic equipment and software installed on a wheeled vehicle to automate the driving control of a car in a traffic stream and systems for information interaction with other road users and elements of the road infrastructure of an intelligent transport system.

the implementation of various scenarios of threats to information interaction between the UV and the ID of urban and main roads. In the process of mandatory testing of digital communications security, the aim of certification is to determine the degree of compliance of the V2X technological platform of the tested UV with the requirements of the national cybersecurity standard) for connected and autonomous vehicles with a driving automation class higher than 3.

Interaction mechanism of an autonomous vehicle with physical and cyber-physical infrastructure is established by the complex use of the following key enabling technologies of smart mobility: a) automation; b) digital user interface; c) information interconnectivity; d) digital data. Each of these technologies has its own profile of risks associated with accidental and intent violation of normal operation mode (use), which must be identified and assessed when certifying the object of analysis of the UV cybersecurity. National certification system for UV cybersecurity should be based on proven approaches for general model of an automated driving system specification, a model of threats from external sources for TP V2X specification and a threat assessment method that are used for assessment and testing during the design and development of a vehicle in accordance with the generally accepted V-type procedure for analyzing safety [12, 13, 14, 15, 16, etc.].

We propose the guidelines for testing the UV cybersecurity for the assessment of the criticality of threats to an automatic (automated) driving system:

- evidentiality, i.e. identification of threats that could be carried out during an attack in real conditions, confirmed by actual cases of attacks with an assessment of the final proof for making a decision on the need for correction (protection method);
- concreteness, i.e. defining clear elements and operations for use in the valuation method;
- operationality, i.e. formation of a workable (practical) procedure for identifying threats that can be established with a focus on the critical path of events leading to serious problems for the safe operation of a highly automated vehicle, to determine the possibility in the process of vehicle development to decide on the composition and priority of measures to protect automated driving system functions.

Analysis of existing approaches (see [17, 18, 19, etc.]) shows that to build a testing model and to ground the verification methodology, it is necessary to proceed from the following approximate composition of active threats of deliberate violation of the UV cybersecurity contour:

1) Vulnerability in the telematics communication unit (TCU) that could be exploited to allow a third party to remotely control the vehicle's TCU or to get access to the electronic control unit (ECU).

2) Vulnerability in the vehicle's entertainment system, which can be exploited by a third party remotely: to determine the location of the vehicle and then switch to the vehicle's remote control mode by invading the vehicle's built-in system from an exploited port of the cellular network and falsifying the controller firmware; unlock the doors of the vehicle by sending a command from the telematics server that is potentially dangerous for road users; to get access to confidential information on the operation of the car: leakage of information about the user ID and password can be used to activate the service settings of control systems; to gain access to confidential information on the operation of the vehicle: leakage of information about the user ID and password can be used to activate the service settings of control systems, etc.

3) Vulnerability in a wireless LAN that could be exploited to allow a third party to remotely control an unmanned vehicle by directing the user to an attacking site using a fake Wi-Fi hotspot or over a public cellular network.

4) Vulnerability in a mobile application that can be exploited to allow a third party to remotely control the settings of the human machine interface (HMI), air conditioner, burglar alarms and other devices via a Wi-Fi access point (DSRC) in a connected or offline car.

5) Vulnerability in a connected service, which can be exploited to allow a third party remotely: to conduct false authentication and control other vehicles during authentication between smartphones and the server API of the user (owner / operator) of the UV; to unlock and open the doors by gaining

access to the UV when the security token used to authenticate smartphone devices expires; enter an unintentional code from a USB port inside the car to distort the autonomous vehicle navigation (AVN) settings, etc.

Let us characterize the problem area and the available testing tools for UVs cybersecurity, determined by the specifics of the main parameters of the V2X technological platform within the ITS.

Objectives, methods and order of certification

The common task of the verification and validation methods for UV solutions is to obtain confirmation that the automated driving system tested for compliance with safety requirements ensures a positive balance of risks in comparison with the characteristics of a human driver, taking into account all possible driving scenarios arising from a noticeable external influence. It is assumed that full testing of each individual threat scenario is not appropriate and technically feasible, therefore an acceptable and practical way to demonstrate / confirm the security of a system is based on a statistical assessment method. And although the experience of the commercial operation of the UV is still insufficient (there are examples of local use in the field of public transport), the accumulated material of laboratory and field tests and experimental operation in limited urban spaces allows us to formulate critical provisions for characterizing the profile of the cybersecurity threats of the UV [20, 21, 22, etc.], as well as even standardize the basic requirements for normative values and methods for assessing cybersecurity during research and certification tests of UV [12, 23, 24, etc.].

For example, in [25], representing the so-called "white paper" in the format used, specialists and experts from leading companies[7] in the intelligent vehicle market formulated an integrated approach to the consideration of topics and problems of automated driving safety, an overview of the basic elements and methods of ensuring the safety of high automated vehicle, as well as the characteristics of the methods of testing the safety[8] of technologies and devices of the UV. Let us characterize the key points of the provisions and recommendations that allow, according to expert estimates, to build, test and operate a safe automated vehicle. When carrying out certification for a UV with automation level 3 and higher, the following main challenges and tasks of security testing can be formulated, which make it possible to identify the degree of compliance of the tested device (object) with the established requirements:

– Objective 1. Statistical demonstration of the system's safety and positive balance of risks without interaction with the driver / operator: here it cannot be assumed that the driver / operator is fully alerted and involved in all scenarios, which implies the need to include statistical justifications in the general reasoning for the safety of the automatic driving system;

– Objective 2. System safety in interaction with the driver / operator (especially when switching / intercepting control maneuvers): the driver / operator must maintain awareness of the mode and receive an unambiguous indication of any mode transitions, and the system must reasonably maintain an effective interception ability to maintain controllability, which defines the requirement to analyze the effects of control interception on the safety of automatic driving;

– Objective 3. Consideration of currently unknown scenarios in traffic: new scenarios are a result of the emergence in a common network environment of risks of situations associated with the operation of a single automated traffic control system, and with interactions between individual automated driving systems and vulnerable road users traffic, which makes it mandatory to test the safety of automatic driving due to changes in the real and virtual world of the road infrastructure (situation);

[7] The companies: Aptiv, Audi, Baidu, BMW, Continental, Daimler, FCA US LLC, HERE, Infineon, Intel and Volkswagen. They constitute the widest and most competent representation in the field of technology and system development, as well as in the production of components and devices for creating BPA.

[8] The focus here is on the development of security components and methods that are required to complement the long-standing and successful commercialized SAE Level 1 (Driver Assistance, DA) and Level 2 (Partial Automation, PA) automation systems. It is important to note that when characterizing SAE Level 3 and higher automated steering systems, the review authors consider the safety of a connected and autonomous vehicle in an electronic communications network environment in two aspects: as security, if it concerns active threats (factors of influence and impact of a predominantly digital environment), and as safety, if it concerns passive threats (factors of influence and impact of a predominantly physical environment).

– Objective 4. Verification of various configurations and variants of the system: since the automatic driving system consists of several elements, it is possible for various reasons (including deliberate unauthorized actions) to arise situations of asynchronous software updates and / or changes in equipment, which implies the need to test increased the number of options for the actual state of settings for assessing the safety of the automatic driving system;

– Objective 5. Validation of systems and subsystems based on machine learning: the functioning of the elements of automated vehicles of the next generations relies on machine learning algorithms when making control / regulatory decisions (for example, recognizing the traffic situation and evaluating actions), therefore, when assessing various impacts on them decomposition into individual components is unacceptable, which requires adapting methods for testing the overall safety of the automatic driving system.

An exemplary set of testing techniques is recommended in ISO 26262: 2018 "Road Vehicles – Functional safety" [26], which is the basis of the current draft international standard (DIS) of the detailed cybersecurity standard for ISU ISO / SAE DIS 21434 "Road Vehicles – Cybersecurity engineering" [27]. Test development methods are classified according to the degree of knowledge about the object under test (OuT). Obviously, the already characterized variability in the control settings and behavior / operation parameters of the FUA level 3 and higher in the digital environment of information communications corresponds to the recommendation specified in ISO 26262. The test design methods are based on:

– scheme-based test design techniques;
– equivalence partitioning test design techniques;
– value test design techniques;
– search-based test design techniques;
– design of experiments;
– mutation test design technique;
– reactive test design technique.

Testing of a UV in the process of its certification (as well as in the process of its design / development), depending on the specific design of the automated driving system, can be carried out with different testing purposes, which predetermines the combination of several test platforms for: a) different stages / areas of verification: individual components – functionality and reliability; integration of automatic driving systems components – static; UV systems in state control – static; UV systems in motion control – dynamic; system of external and internal communications BPA – human-machine interface; UV systems in the active environment of DI ITS; b) various test conditions: laboratories (software in loop, SiL; hardware in loop, HiL; driver in loop, DiL); closed polygon; open road.

Thus, checking the compliance of an intelligent vehicle with the cybersecurity requirements of the used TP UV-DI is a multi-level and multi-stage process. However, within the framework of state control, testing strategies with an emphasis on the entire automatic driving system should be used for mandatory verification of the safety level of the developed or operated UV as a whole.

It is obvious that the necessary technical base and professional competencies for certification can be organizationally and geographically distributed, which predetermines the need to optimize the structure of the construction and regulation of the functioning of the national certification system for BPA.

Structure, regulations and certification mechanism

The goals and functions of certification determine the structure of the national certification system: the state certification body for UV (with subdivisions of the federal, regional and local levels of authority and responsibility); accredited certification bodies, accredited testing laboratories. The subject and object of certification determine the inspection procedure: the conformity assessment procedure – declarative; types of tests performed – selective (components and devices) and complete (products and complexes), prototypes and serial products; types of official documents on the assessment of the char-

acteristics of the cybersecurity of UV – test report, preliminary conclusion and certificate of conformity. The tasks and methods of certification determine the verification mechanism: the testing scheme should provide for both sanctions (manufacturer / importer: certification for the admission of UV and individual components of the automatic driving system to the UV market, first introduced to the consumer market and in the field of commercial / official transport services, including maintenance and repair of components vulnerable from the point of view of cybersecurity), and periodic inspection control (owner / operator: confirmation of the safety of products that have already passed the certification procedure and are allowed to operate – similar to the procedure for regular state technical inspection of vehicles for their admission to operation and the conclusion of appropriate insurance obligations).

The basic principle of building a certification system and conducting any certification tests is the independence of the testing laboratory, which conducts testing, and the certifying organization, which further monitors the results of the tests carried out by the laboratory. At the same time, the state certification body carries out a regular external audit[9] of the activities of the certifying organization and testing laboratories, assessing the completeness and quality of their functions, which, if gross and / or systematic violations are detected, may lead to the suspension and revocation of licenses, and the cancellation of accreditation certificates.

To fully reveal the ITS potential and effectively counteract the emerging cybersecurity threats, it is necessary to clearly and strictly coordinate the activities of all actors in the design and development, production and operation of BPA. The problems they face are complex, therefore, on the part of the state, certain efforts are required to concentrate professional competencies when developing the institutional framework for certification activities in the field of UV, as well as organizing the training of qualified specialists and creating a technical base for operators of the regulatory mechanism of this market.

It is obvious that the UV cybersecurity entirely depends on the competence and responsibility of the subject conducting the tests. It is important that the existing capabilities of domestic engineering centers, research laboratories and test sites are used to create a network of testing laboratories for the national certification system. The key tasks, in our opinion, are:

– determination of requirements for the operator of the certification services market (critical parameters: availability of competent personnel, availability and condition of test platforms for assessing the characteristics of equipment (hardware, HW) and programs (software, SW) for ITS from the standpoint of compliance with the characteristics of UV cybersecurity;

– development of a procedure for accreditation / certification of authorized certification organizations and testing laboratories: the use of a state control tool in the field of cybersecurity ITS is important for regular monitoring of the competence and equipment of market participants in the certification of UV;

– substantiation of the economic model of the UV certification process: the tariffs for certification and testing services should be determined differentially based on the type of UV, TP parameters of the information and communication interaction between the UV and the ID and the market capacity for the tested type of UV, as well as depend on the set of tests performed (coverage of current costs) and applied test platforms (covering investment costs for the necessary periodic modernization of test platforms and maintaining a high technical level of the tools for assessing compliance with the requirements of UV and ITS cybersecurity in connection with the rapid pace of innovation in the IT sphere).

Of course, the considered aspects of UV certification do not cover all issues of ensuring cybersecurity in the ITS environment and do not provide an exhaustive description of the problem of testing compliance with TP UV-DI. However, the arguments and formulated provisions can be used to justify organizational decisions and form the basic requirements of technological regulations for assessing condition and control of UV admission to operation on public roads.

[9] In addition, the state certification body, in the event of incidents at the facilities, requests from consumers of certification services, or receiving requests from law enforcement agencies in accordance with the established procedure, related to the leakage of confidential and sensitive information about applicants and certification objects, may inspect certification organizations and testing laboratories.

Results, conclusions and recommendations

The study made it possible to identify the key problems and formulate the main issues of building a national cybersecurity certification institute within the framework of the ITS being created with the expanding scope of application of unmanned vehicles.

From our point of view, the complex of works to create a certification system for UV within the framework of ITS should include the following areas: improving the legal base for the verification and validation of systems and technologies for ITS; developing the functionality of the state certification agency and its territorial infrastructure; creation of a mechanism for licensing, accreditation and certification of participants in the testing process; organization of design, development and production of national software-hardware complexes for test platforms evaluating the level of cybersecurity of V2X technologies.

There are two approaches in the legal field of Russian legislation that are used to certify cybersecurity tools in the field of ITS based on the corresponding types of regulatory documents:

– Functional testing of UV identifying the fact of implementation of the declared functions by the checked object (product-product or technology) of the ITS. This testing is most often carried out for compliance with a specific regulatory document[10] – technological regulations. In some cases, in the absence of a document establishing the regulatory characteristics for cybersecurity for a certified object, the necessary functional requirements are formulated in the form of technical conditions or technical specifications (in accordance with the provisions of the GOST R 15408 standard).

– Structural testing of the program code used in the UV (HW and SW automatic driving systems and digital communications), which determines the absence of undeclared capabilities. That is, there is an identification of software tabs which initiate the performance of functions that are not declared and not described in the documentation to the components / devices of the UV upon the occurrence of certain conditions or when external authorization is carried out, which allows unauthorized influences on the monitoring and control information and, therefore, on the operating modes of the UV (in accordance with the provisions of the standard GOST R 51275-99).

The general organization of the certification process in accordance with common approaches and established practices in the regulatory area can be as follows:

1. The applicant submits an application to the federal / territorial certification agency for certification tests of the UV cybersecurity (component of automatic driving systems and digital communications).

2. The state certification agency determines the accredited certifying organization and testing laboratory for testing the UV cybersecurity.

3. The testing laboratory together with the applicant determines the testing plan[11].

4. The certifying organization and the applicant enter into a contract for the provision of certification services based on the agreed composition and cost of certification work.

5. The testing laboratory, as a co-contractor of the contract, conducts certification tests of selected product samples provided by the applicant in accordance with the selection rules for a full range of test and assessment works to confirm compliance with the UV cybersecurity requirements, including identification and analysis of documents submitted by the applicant.

[10] For instance, the Federal Service for Technical and Export Control of the Russian Federation (until 2004, the State Technical Commission of Russia) established such guidelines for firewalls and means of protection against unauthorized access (see: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-). In addition, for commercial software products, one can note the requirements for source code security auditing contained in the international standards PA DSS, PCI DSS and NISTIR 4909 (see: https://www.aadyasecurity.com/what-is-security-compliance- and-why-should-you-care).

[11] The test plan based on the accepted application includes the main certification conditions: certification scheme; regulatory documents on the basis of which certification will be carried out; information about the expert organization that will analyze the state of production, if provided by the certification scheme; the procedure for selecting samples of components / products for testing; the procedure for testing samples of components / products; the procedure for assessing the conditions for the production of components / products and the characteristics of information security of the developed (prototype) or operated (industrial design) BPA; criteria for assessing the compliance of UV cybersecurity with the requirements of technological regulations (state standard); the procedure for providing, if necessary, additional documents confirming the safety of components / products that are used in the BPA for operation in the environment of the national ITS.

6. On the basis of the protocols with the test results the testing laboratory prepares: a) preliminary conclusions on conformity (during a separate stage or one of the full cycles of cybersecurity testing), if certain inconsistencies with the established / declared requirements are revealed, which can be eliminated by the applicant in the course of work; b) the final conclusion (upon completion of the work plan for testing the object of verification provided by the applicant).

7. Test materials are transferred to the federal / territorial certification agency for an independent examination of the results of testing the UV cybersecurity (independent examination is carried out with the participation of at least two licensed expert organizations, which must confirm both the completeness and correctness of the tests, and the validity of the formulated conclusions and recommendations).

8. On the basis of the conclusion of the certifying organization within the established regulatory period (for example, 30 days) the state certification agency: draws up a certificate of conformity for the test object; organizes, in case of revealing any potentially removable inconsistencies, an additional examination with a change in the composition of the involved accredited certification organizations and testing laboratories; decides on the refusal to issue a certificate, providing the applicant with an act of work performed and a conclusion with justification of the identified discrepancies of the UV (components / products of automatic driving systems and digital communications) in terms of cybersecurity.

The transition to mass industrial and personal use of UV and the creation of a national certification system for assessing cybersecurity for TP UV-DI presupposes an introduction of significant changes and extensions of Russian legislation, including the correction of certain norms of the civil, administrative and criminal codices of the Russian Federation. First of all, we point out that in accordance with the provisions of Article 25 of the Federal Law No. 184-FZ "On Technical Regulation" dated 27.12.2002 (as amended on November 28, 2018), the equipment used and the services provided in this sphere should be included in the Unified list of products subject to mandatory certification[12], they require mandatory confirmation of compliance with the established safety requirements and quality characteristics should as determined in the technological operating regulations.

Here, it is important to ensure interdepartmental and inter-organizational interaction in the field of standardization of the development and operation of UV. It should be noted that the general functions of accreditation are concentrated in the Rosaccreditation[13] of the Ministry of Economic Development of the Russian Federation, which currently has 6 territorial agencies in federal districts. Taking into account the specifics of the task of assessing the vulnerabilities of information interaction within the TP UV-DI, it is necessary to choose an organizational form of cooperation between the Ministry of Transport of the Russian Federation (Federal Service for Supervision in Transport, Rostransnadzor) and the Ministry of Internal Affairs of the Russian Federation (State Inspectorate for Road Safety, Traffic Safety Inspectorate) with authorized state agencies in the field of cybersecurity: the Federal Security Service of the Russian Federation (Center for Licensing, Certification and Protection of State Secrets, CLCPSS FSB of Russia) and the Ministry of Defense of the Russian Federation (Federal Service for Technical and Export Control, FSTEC of the Ministry of Defense of Russia), which have the necessary powers and capabilities to assess the compliance of inspected objects with cybersecurity requirements. The main forms and mechanisms of certification for most of the cybersecurity means (SIS) and software

[12] Decree of the Government of the Russian Federation No. 982 "On approval of the unified list of products subject to mandatory certification and the unified list of products, the conformity of which is confirmed in the form of a declaration of conformity" dated 01.12.2009 (revised on July 4, 2020).

[13] The Federal Service for Accreditation (Rosaccreditation) is a federal executive organization performing the functions of the national accreditation body of the Russian Federation. Rosaccreditation was established in 2011 in accordance with the Decree of the President of the Russian Federation dated 24.01.2011 No. 86 "On the Unified National Accreditation System" and operates on the basis of the Regulations on the Federal Accreditation Service, approved by the decree of the Government of the Russian Federation "On the Federal Accreditation Service" dated 17.10.2011 No. 845 (revised on 23.03.2020). Rosaccreditation is administered by the Ministry of Economic Development of the Russian Federation. The sphere of activity of Rosaccreditation is: formation of a unified national accreditation system; control over the activities of accredited persons. In addition to information security tools, FSTEC also checks IT systems that store personal data: servers and networks of companies or cloud storages. This verification procedure is called the attestation of IT systems, carried out in accordance with the standards of the security levels of the Federal Law "On Personal Data" dated 27.07.2006, No. 152-FZ (revised on 20.04.2020).

are the certification systems for the CLCPSS of the FSB of Russia and the FSTEC of the Ministry of Defense of Russia. The FSB (CLCPSS) certification is intended for testing software subsystems that use cryptographic protection (in the Russian Federation, only national crypto protection algorithms are allowed). The requirements of the FSB certification systems are not public; familiarization with them requires special approvals. The MO (FSTEC) certification is intended to verify the technical protection of information by non-cryptographic methods. The requirements of the FSTEC certification system are open and published on the official website.

The policy in the field of accreditation of certifying organizations and testing laboratories for checking the requirements and certification of TP AV-DI should be determined with the participation of specialized units of the Ministry of Transport of the Russian Federation (Department of State Policy in the Field of Automobile and Urban Passenger Transport, Department of State Policy in the Field of Road Facilities, Department of Transport security and special programs), as well as taking into account the experience and specifics of functioning in the digital environment of traffic management centers (TMS) of public legal entities of the Russian Federation, in the territories of which the infrastructure of the national ITS will be deployed. For the organization of testing of the TP UV-DI cybersecurity, the existing experience of work on certification of technical devices of ensuring transport security in terms of technical devices / systems of inspection and intelligent video surveillance, used during the regular state technical inspection of vehicles, can be used. On March 30, 2017, the Decree of the Government of the Russian Federation No. 969 "On approval of the requirements for the functional properties of technical devices providing transport security and the Rules for mandatory certification of technical devices providing transport security" dated 26.09.2016 came into force, in accordance with which mandatory certification of technical devices providing transport security within the framework of periodic inspection of the condition of wheeled vehicles for various purposes, general requirements for them have been established, and the responsibility for their certification is assigned to the FSB of Russia. It is reasonable to assume that with the expansion of the scope of certification in the field of ITS, the accreditation of certifying organizations and testing laboratories for testing UV cybersecurity can also be entrusted to the CLCPSS FSB of Russia.

Conclusion

Expanding the range of automated functions or systems in vehicles has become a general trend in the use of modern advances in science and technology. While the original primary motivation was to make driving easier and the ride more comfortable, the next steps to automate driving are already focused on reducing fuel consumption and environmental impact, while improving driving safety. At the same time, it is obvious that automated driving and autonomous vehicle movement is a very difficult control task, therefore, replacing a human driver with a computer is a real problem from a technical, organizational and legal point of view.

Due to the emergence of new electronic components, the increased complexity of on-board electronic devices for automated driving and digital communications, the widespread use of intelligent technologies for automated traffic control and the rich information interaction of the vehicle with the external road environment, the safety of transport systems is affected in two ways. On the one hand, machine vision and artificial intelligence technologies can reduce the risks of road accidents involving UV. On the other hand, the range of threats associated with a possible violation of the functional integrity and operability of the UV due to intentional impacts on the electronic components of the automated driving system of the vehicle and its information and communication interaction with the road infrastructure, including traffic control centers within the ITS, is expanding.

This requires improvement of the norms and requirements of the legal and technical regulation of the creation and operation of connected and automated vehicles (CAVs) for various purposes on sections of roads of local and common use, which implies the expansion of the scope and tasks of testing the safety

of public, personal, commercial and special vehicles, including by checking cybersecurity during validation and verification of devices / technologies of the UV and ITS components.

From the standpoint of integrated security in the development of unmanned vehicles for various environments (ground, air and water), it is essential to build a national certification system for systems and technologies ensuring the security of a technological platform for information interaction of UV with the surrounding infrastructure of the organization of automated (connected and autonomous) traffic in digital environment.

The issues discussed in this article make it possible to reveal the importance of the national certification system for ITS components and technologies both from the standpoint of ensuring road safety and digital sovereignty of the Russian Federation in the global network of automotive communications. This includes supporting projects for the restoration of national microelectronics through the formation of sustainable demand for electronic and element base for technical solutions of critical information infrastructure in one of the large-scale and significant sectors of the Russian economy. One of the most important areas for further research and development, in our opinion, should be the improvement of the methodological support for the design of test platforms for control of the safety of UVs for test sites and laboratories, as well as the development of comprehensive testing tools for assessing compliance with the cybersecurity requirements of unmanned vehicles in various modes / operation conditions [27, 28, 29, 30, etc.]. This will make it possible not only to ensure an approximation to the best world practices and trends in the development of end-to-end technologies for unmanned vehicles and the creation of a national mechanism to support innovation [31], but also make the formation of intelligent transport systems in the context of the digital transformation of society an effective and safe means of optimizing and accelerating logistics processes in solving strategic problems of sustainable socio-economic development of the Russian Federation.

REFERENCES

1. Autonomous Driving. Technical, Legal and Social Aspects / Eds. M. Maurer, J. Gerdes, B. Lenz, H. Winner. Berlin, Springer, 2016, 706 p.

2. L**.F. Kazanskaya, N.V. Savitskaya, P.P. Kamzol,** Prospects for the development of unmanned vehicles in Russia. Bulletin of scientific research results, 2018, no. 2, pp. 18–28. (rus)

3. **V.B. Betelin,** On the problem of import substitution and the model of economic development in Russia. Strategic priorities, 2016, no. 1 (9), pp. 11–21. (rus)

4. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. SAE International, 2016. URL: http://standards.sae.org/j3061_201601/ (accessed July 12, 2020).

5. **L.K. Tereshchenko, Yu.A. Tikhomirov, T.Ya. Khabrieva,** The concept of legal support for technical regulation. Journal of Russian Law, 2006, no. 9. pp. 3–17. (rus)

6. **A.Yu. Mkhitaryan, Yu.I. Mkhitaryan,** Constitutional and legal basis for mandatory certification of works (services) in the Russian Federation. Age of quality, 2019, no. 2, pp. 8–18. (rus)

7. **E.E. Nikolaeva, T.V. Azarova,** On the issue of competition as an institution. Modern high technologies. Regional Supplement, 2016, no. 3 (47), pp. 132–140. (rus)

8. **A.S. Markov, Yu.V. Rautkin,** Certification of information security tools in accordance with information security requirements: new paradigm, Information and mathematical technologies in science and management, 2016, no. 1 (27), pp. 94–102. (rus)

9. **C. McDermott, G. O'Connor,** Managing radical innovation: an overview of emergent strategy issues. Journal of Product Innovation Management, 2002, no. 19 (6), pp. 424–438.

10. **W. Eversheim,** Innovation Management for Technical Products. Berlin Heidelberg: Springer Verlag, 2009. 444 p.

11. **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.

12. **W. Huang, K. Wang, Y. Lv, F. Zhu,** Autonomous Vehicles Testing Methods Review. IEEE 19th International Conference on Intelligent Transportation Systems, 2016, pp. 163–198. URL: https://www.researchgate.net/publication/311919670_Autonomous_vehicles_testing_methods_review (accessed September 12, 2020).

13. **C. Schmittner, Z. Ma, C. Reyes, O. Dillinger, P. Puschner,** Using SAE J3061 for Automotive Security Requirement Engineering. International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2016). SAFECOMP Workshops, 2016, pp. 157–170.

14. **Z. Ma, C. Schmittner,** Threat Modeling for Automotive Security Analysis. Advanced Science and Technology Letters, 2016: 139, pp. 333–339.

15. **C. Schmittner, Z. Ma, T. Gruber,** Standardization Challenges for Safety and Security of Connected, Automated and Intelligent Vehicles 3rd International Conference on Connected Vehicles & Expo (ICCVE 2014), 2014, pp. 941–942.

16. **A. Joshi, M. Heimdahl, S.P. Miller, M. Whalen,** Model-Based Safety Analysis. NASA, CR-2006-213953, 2006. Hampton: National Aeronautics and Space Administration, 2006. 60 p.

17. **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.

18. **M. Rosenquist,** Prioritizing Information Security Risks with Threat Agent Risk Assessment. Intel Corp. 2009. URL: https://communities.intel.com/servlet/JiveServlet/download/4693-1-3205/Prioritizing_Info_Security_Risks_with_TARA.pdf (accessed September 12, 2020).

19. **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. URL: http://www.sip-adus.go.jp/file/rd-result_all.pdf (accessed September 12, 2020).

20. **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.

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

22. PEGASUS Method – An Overview, 2019. URL: https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/PEGASUS-Gesamtmethode.pdf (accessed September 12, 2020).

23. **M. Joerger, C. Jones, V. Shuman,** Testing connected and automated vehicles (CAVs): Accelerating innovation, integration, deployment and sharing results. In. Road vehicles Automation 5, eds.: Meyer G., Beiker S. Shpringer, 2019, pp. 197–206.

24. Safety first for automated driving: a white paper / Aptiv Services US, LLC; AUDI AG; Bayrische Motoren Werke AG; Beijing Baidu Netcom Science Technology Co., Ltd; Continental Teves AG & Co oHG; Daimler AG; FCA US LLC; HERE Global B.V.; Infineon Technologies AG; Intel; Volkswagen AG. 2019. 146 p.

25. ISO 26262-1:2011. Road vehicles – functional safety. International Organization for Standardization, Geneva, Switzerland. 2011.

26. ISO/SAE DIS 21434: 2020. Road vehicles – Cybersecurity engineering. International Organization for Standardization, Geneva, Switzerland. Society of Automotive Engineers International, Warrendale, USA. 2020.

27. **Z. Szalay, T. Tettamanti, D. Esztergar-Kiss, I. Varga, C. Bartolini,** Development of a test track for driverless cars: vehicle design, track configuration, and liability considerations. Periodica Polytechnica Transportation Engineering, 2018: 46(1), pp. 29–35.

28. **H. Peng,** MCity ABC Test: A Concept to Assess the Safety Performance of Highly Automated Vehicles. University of Michigan, 2019. 15 p.

29. **R. Chen, M. Arief, W. Zhang, D. Zhao,** How to Evaluate Proving Grounds for Self-Driving? A Quantitative Approach. arXiv preprint, arXiv: 1903.08352, 2019. Elektronnyy resurs URL: https://arxiv.org/pdf/1909.09079.pdf (accessed September 12, 2020).

30. **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 areas. Scientific and technical statements of SPbSPU. Economic sciences, 2020, no. 5, pp. 3–23. (rus)

31. **G.N. Makhmudova, A.V. Babkin,** Theoretical aspects of innovative development in the context of economic modernization: trends, analysis and prospects // Scientific and technical bulletin of SPbSPU. Economic sciences. 2020. Vol. 13, No. 2. P. 40–52. (rus)

СПИСОК ЛИТЕРАТУРЫ

1. Autonomous Driving. Technical, Legal and Social Aspects / Eds. M. Maurer, J. Gerdes, B. Lenz, H. Winner. Berlin, Springer, 2016, 706 p.

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

3. **Бетелин В.Б.** О проблеме импортозамещения и альтернативной модели экономического развития России. Стратегические приоритеты, 2016, № 1 (9), С. 11–21.

4. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems. SAE International, 2016. URL: http://standards.sae.org/j3061_201601/ (accessed July 12, 2020).

5. **Терещенко Л.К., Тихомиров Ю.А., Хабриева Т.Я.** Концепция правового обеспечения технического регулирования. Журнал российского права. 2006. №. 9. С. 3–17.

6. **Мхитарян А.Ю., Мхитарян Ю.И.** Конституционно-правовая основа обязательной сертификации работ (услуг) в Российской Федерации. Век качества. 2019. № 2. С. 8–18.

7. **Николаева Е.Е., Азарова Т.В.** Современные наукоемкие технологии. Региональное приложение. 2016. № 3 (47). С. 132–140.

8. **Марков А.С., Рауткин Ю.В.** Сертификация средств защиты информации по требованиям безопасности информации. Новая парадигма // Информационно-математические технологии в науке и управлении, 2016, № 1 (27), с. 94–102.

9. **McDermott C., O'Connor G.** Managing radical innovation: an overview of emergent strategy issues. Journal of Product Innovation Management, 2002. № 19 (6), pp. 424–438.

10. **Eversheim W.** Innovation Management for Technical Products. Berlin Heidelberg: Springer Verlag, 2009. 444 p.

11. **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.

12. **Huang W., Wang K., Lv Y., Zhu F.** Autonomous Vehicles Testing Methods Review. IEEE 19th International Conference on Intelligent Transportation Systems, 2016, pp. 163–198. URL: https://www.researchgate.net/publication/311919670_Autonomous_vehicles_testing_methods_review (accessed September 12, 2020).

13. **Schmittner C., Ma Z., Reyes C., Dillinger O., Puschner P.** Using SAE J3061 for Automotive Security Requirement Engineering. International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2016). SAFECOMP Workshops, 2016, pp. 157–170.

14. **Ma Z., Schmittner C.** Threat Modeling for Automotive Security Analysis. Advanced Science and Technology Letters, 2016: 139, pp. 333–339.

15. **Schmittner C., Ma Z., Gruber T.** Standardization Challenges for Safety and Security of Connected, Automated and Intelligent Vehicles 3rd International Conference on Connected Vehicles & Expo (ICCVE 2014), 2014, pp. 941–942.

16. **Joshi A., Heimdahl M., Miller S.P., Whalen M.** Model-Based Safety Analysis. NASA, CR-2006-213953, 2006. Hampton: National Aeronautics and Space Administration, 2006. 60 p.

17. **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.

18. **Rosenquist M.** Prioritizing Information Security Risks with Threat Agent Risk Assessment. Intel Corp. 2009. URL: https://communities.intel.com/servlet/JiveServlet/download/4693-1-3205/Prioritizing_Info_Security_Risks_with_TARA.pdf (accessed September 12, 2020).

19. **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. URL: http://www.sip-adus.go.jp/file/rd-result_all.pdf (accessed September 12, 2020).

20. **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.

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

22. PEGASUS Method – An Overview, 2019. URL: https://www.pegasusprojekt.de/files/tmpl/Pegasus-Abschlussveranstaltung/PEGASUS-Gesamtmethode.pdf (accessed September 12, 2020).

23. **Joerger M., Jones C., Shuman V.** Testing connected and automated vehicles (CAVs): Accelerating innovation, integration, deployment and sharing results. In. Road vehicles Automation 5, eds.: Meyer G., Beiker S. Shpringer, 2019, pp. 197–206.

24. Safety first for automated driving: a white paper / Aptiv Services US, LLC; AUDI AG; Bayrische Motoren Werke AG; Beijing Baidu Netcom Science Technology Co., Ltd; Continental Teves AG & Co oHG; Daimler AG; FCA US LLC; HERE Global B.V.; Infineon Technologies AG; Intel; Volkswagen AG. 2019. 146 p.

25. ISO 26262-1:2011. Road vehicles – functional safety. International Organization for Standardization, Geneva, Switzerland. 2011.

26. ISO/SAE DIS 21434: 2020. Road vehicles – Cybersecurity engineering. International Organization for Standardization, Geneva, Switzerland. Society of Automotive Engineers International, Warrendale, USA. 2020.

27. **Szalay Z., Tettamanti T., Esztergar-Kiss D., Varga I., Bartolini C.** Development of a test track for driverless cars: vehicle design, track configuration, and liability considerations. Periodica Polytechnica Transportation Engineering, 2018: 46 (1), pp. 29–35.

28. **Peng H.** MCity ABC Test: A Concept to Assess the Safety Performance of Highly Automated Vehicles. University of Michigan, 2019. 15 p.

29. **Chen R., Arief M., Zhang W., Zhao D.** How to Evaluate Proving Grounds for Self-Driving? A Quantitative Approach. arXiv preprint, arXiv: 1903.08352, 2019. Электронный ресурс URL: https://arxiv.org/pdf/1909.09079.pdf (accessed September 12, 2020).

30. **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

31. **Махмудова Г.Н., Бабкин А.В.** Теоретические аспекты инновационного развития в условиях модернизации экономики: тенденции, анализ и перспективные возможности // Научно-технические ведомости СПбГПУ. Экономические науки. 2020. Т. 13, № 2. С. 40–52. DOI: 10.18721/JE.13204

Статья поступила в редакцию 01.03.2021.

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

КУРГУЗОВ Василий Борисович
E-mail: kurguzov@rosdornii.ru
KURGUZOV Vasiliy V.
E-mail: kurguzov@rosdornii.ru