Information security in the field of transport services

Nina Semeryanova[1*], and *Alexander* Mordvinov [2]

[1] South Ural State University (National Research University), Nizhnevartovsk Branch, Mira str., 9, 628600, Russia
[2]Tyumen Industrial University, Volodarskogo str., 38, Tyumen, 625000, Russia

Abstract. The relevance of the issue under study is associated with the use of information and telecommunication technologies in the transport industry and ensuring the information security of the data obtained in the digitalization of Russian economy. The study is purposed to monitor legislation and analyze measures aimed at protecting information security in the transport industry. The novelty of the study lies in the formulation, justification and solution of the issues of ensuring information security by filling in the gaps in legislative regulation and organizing effective interaction of transport structures. The leading research approach includes such scientific methods as dialectics, analysis, synthesis, deduction, comparative legal and formal legal method. The analysis can contribute to the formation of a stable legislative regulation on ensuring information security in the transport industry. The paper substantiates the need to build a single coordination system of interaction "state - subject of the federation - municipality - enterprise", as well as establishment of communication between transport enterprises.

1 Introduction

Transport industry is a special sector of the economy that plays an important role in the development of states. According to experts of the Organization for Economic Cooperation and Development, by 2030, the investment needs of global transport infrastructure, including air and sea ports, railways, and pipelines, will amount to 11.3 trillion dollars. It is estimated that more than 44% of this volume should be invested in railway infrastructure (about 5 trillion dollars). According to the “Analysis of the Road Freight Transport Market in Russia”, prepared by BusinesStat in 2019, in 2018 the cost volume of Russian market of commercial road transport increased by 7.7% and amounted to 814.9 billion rubles. This is due to the growth in cargo turnover, which in 2018 amounted to 139.5 billion ton-km, which exceeded the level of 2017 by 5%. The increase in traffic is ensured by development of various services of the fleet management system of vehicles and telemetry facilities. Transport management is based on the use of intelligent transport and logistics systems. One of the most promising directions in the development of digital services in the transport industry is geo-information technology, which is used not only to monitor traffic, but also

[*]Corresponding author: nina_777s@mail.ru

to equip vehicles with touch sensors that read information from surrounding objects and transmit it to a single center for processing information and monitoring the transportation process.

According to Deputy Prime Minister and Chairman of the Government Commission on the Digital Economy Maxim Akimov, digitalization of transport industry can increase its efficiency by 35%. Global changes in organization and implementation of transportation of goods, passengers and baggage associated with introduction of digital technologies in the transport turnover are fundamentally changing socio-economic relations in Russia. Intelligent technologies used in the transport sector open up a completely different scale of vision for this service sector - these are smart cars and smart cities, their interaction between themselves and the world around them, their special place in the system of the present-future digital economy. A striking example of changing relationship is the use of self-driving cars that exchange information about the road traffic situation with a single managing center, as well as between themselves. However, in addition to the positive economic effect, digitalization of the transport industry brings a number of serious issues. This is, for example, information security of data. In this regard, scientists are facing an important issue - ensuring protection of information resources.

Theoretical basis of the study was made by scientific works in the field of information law, devoted to general theoretical problems, written by scholars such as O.A. Gavrilov, D.V. Gribanov, S.Ya. Kazantsev, V.A. Kopylov, M.A. Lapina, A.B. Minbaleev, C. B. Molchanov, I.L. Petrukhin, V.A. Severin, A.A. Tedeev, A.A. Fatyanov et al. Studies in the field of legal regulation of the institution of personal data and their protection were carried out by F.A. Abaev, N.G. Belyaev, A.L. Dokhodov, V.P. Ivansky, H.H. Kuftin, A.A. Malyuk, E.A. Mindrova, A.B. Morozov, O.B. Prosvetova, D.Yu. Pisarev, A.G. Sabanov, O.S. Sokolova, A.V. Kucherenko and others

The issues of functioning of the information security system from the perspective of technical sciences are reflected in the works of A.L. Balyberdina, V.A. Gerasimenko, A.A. Grusho, E.V. Kaspersky, V.D. Kurushina, A.A. Malyuka, V.E. Potanina, A.P. Fisuna and others. Providing information security in transport involved such scientists as Yu.V. Zvorykina, V.V. Glushchenko, A.V. Bukaeva D.V. Gontar, V.V. Motin et al.

The empirical basis was constituted by regulatory legal acts of international law and Russian legislation. The provisions on information protection are enshrined in the Federal Law of July 27, 2006 No. 149-FZ (as amended on March 18, 2019) “On Information, Information Technologies and Information Protection”. So, paragraph 1 of Art. 4 establishes that the legislation of the Russian Federation on information, information technologies and information protection is based on the Constitution of the Russian Federation, international treaties of the Russian Federation and consists of this Federal Law and other regulatory relations for the use of information of federal laws. Art. 16 of this law establishes following legal regime for the protection of information: ensuring the protection of information from unauthorized access, destruction, modification, blocking, copying, provision, distribution, as well as from other illegal actions in relation to such information; maintaining confidentiality of information with restricted access; realization of the right to access information. State regulation of relations in the field of information protection is carried out by establishing requirements for information protection, as well as liability for violation of the legislation of the Russian Federation on information, information technologies and information protection.

The holder of the information, the operator of the information system, in cases established by the legislation of the Russian Federation, is obliged to ensure: prevention of unauthorized access to information and (or) its transfer to persons who do not have the right to access information; timely detection of unauthorized access to information; warning of the possibility of adverse consequences of violation of the procedure for access to

information; prevention of impact on technical means of information processing, resulting in disruption in their functioning; possibility of immediate recovery of information modified or destroyed due to unauthorized access; continuous monitoring of the level of information security; finding on the territory of the Russian Federation of information databases used for collection, recording, systematization, accumulation, storage, updating (changing), extraction of personal data of citizens of the Russian Federation are carried out.

The Board of the Eurasian Economic Commission was actively involved in this issue and presented a list of standards and recommendations in the field of information security that are used as part of implementation of the digital agenda of the Eurasian Economic Union [1], in particular, section IV of this document provides for protection of information using cryptographic protection means: Transport Layer Security (TLS) Protocol Version 1.2: RFC 5246, transport Layer Security (TLS) Protocol Version 1.3: RFC 8446, as well as recommendations on standardization P 1323565.1.020-2018 "Information technology. Cryptographic information security. The use of cryptographic algorithms in the transport layer security protocol (TLS 1.2). " STB 34.101.45-2013 “Information technology and security. Algorithms for electronic digital signature and key transport based on elliptic curves. " STB 34.101.65-2014 “Information technology and security. Transport Layer Security Protocol (TLS)».

Legal regulation in the field of transport security is carried out by the Federal Law dated 09.02.2007 No. 16-FZ (as amended on 02.08.2019) “On Transport Security” (amended on 08.08.2019). In Art. 11, issues of information security of transport are regulated, in accordance unified state information system for ensuring transport security is created, which is the property of the Russian Federation. A separate link in the information system is automated centralized databases of personal data on passengers and personnel of vehicles. Automated centralized databases of personal data on passengers and personnel (crew) of vehicles are formed on the basis of information provided by transport infrastructure entities and carriers, federal executive bodies, foreign states and organizations in the framework of international cooperation on transport security. The information resources of the unified state information system for ensuring transport security are limited access information. The procedure for formation and maintenance of automated centralized databases of personal data on passengers and personnel (crew) of vehicles, as well as provision of the data contained in them, is established by the federal executive body authorized by the Government of the Russian Federation.

A transport infrastructure entity or a carrier from a foreign state who owns a vehicle that carries out international passenger transportation to the Russian Federation, from the Russian Federation and (or) through the territory of the Russian Federation, or who use it on other legal grounds, must ensure the transfer of data to automated centralized databases personal data on passengers and personnel of vehicles in accordance with the Federal Law of July 27, 2006 No. 152-FZ “On personal data ”, Federal Law “On Transport Security”, unless otherwise provided by international treaties of the Russian Federation. Verification of compliance with the procedure for the transfer of information is carried out by the authorized federal executive body in the field of transport security.

In order to ensure a mechanism for implementing legislation on information security, the Departmental Target Program of the Ministry of Transport of the Russian Federation “Digital Platform of the Transport Complex of the Russian Federation” has been developed; its implementation period is 2019 - 2024. The total funding of the event “Development of a unified state information system for ensuring transport security, including automated centralized databases of personal data on passengers and personnel of vehicles” from the federal budget is estimated at 1,208,584.63 thousand rubles, including: for 2019 - 192 571.30 thousand rubles; for 2020 - 192 571.30 thousand rubles; for 2021 -

193,912.40 thousand rubles; for 2022 - 201,668.90 thousand rubles; for 2023 - 209 735.65 thousand rubles; for 2024 - 218 125.08 thousand rubles.

In August 2019, a working group on the development of the concept of digital transformation began work at the Department of Information Technologies and Digital Development of Ugra as a part of the implementation of state tasks in the field of information security. It was composed of representatives of various authorities, which will determine direction of digital transformation of the region, develop proposals for a draft concept and a plan for its implementation. These topics became key topics during the strategic session. The session was attended by representatives of the authorities of the Autonomous Area, the business community and the World Bank, whose experts provide advice on the development of the concept.

Digital industry is not a new topic for the Khanty-Mansiysk Autonomous Area - Ugra. The district has the state program "Digital Development of the Khanty-Mansiysk Autonomous Area - Ugra", approved by the Government of the Khanty-Mansi Autonomous Area-Ugra, No. 353-p dated 10/05/2018. The purpose of the state program is to create an information space based on the use of information and telecommunication technologies to improve the quality of life of citizens, improve the working conditions of organizations of the Khanty-Mansiysk Autonomous Area - Ugra and provide conditions for the implementation of an effective management system in government bodies of the Khanty-Mansiysk Autonomous Area - Ugra . One of the provisions of this program is to reduce the average downtime of state and municipal systems as a result of computer attacks from 48 to 1 hour. In the field of transport services, it is planned to develop RNIS for continuous remote monitoring of the current location of vehicles, the state of operation of systems and equipment based on sensor readings, monitoring compliance with drivers' work and rest, monitoring the road transport network in order to improve transport safety, quality of transport services, effectiveness of monitoring their quality, economic efficiency of the operation of automobile vehicles for various purposes, effectiveness of transport management processes.

2 Methods

Theoretical aspects of the issues of legal regulation considered by such authors as E.B. Belov, V.P. Elk, G.V. Krasnova, A.A. Markov and others made it possible to determine the complex nature of the concept of "information security", which includes the presence of threats of an internal and external nature. The dialectical method allowed a comprehensive study of the essence of the existing contradictions.

The comparative legal method made it possible to correlate federal legislation with the developing legislation of the region in the transport sector, and to identify gaps in legislative regulation.

3 Results

Monitoring of federal legislation and regional regulatory legal acts of the Khanty-Mansiysk Autonomous Area-Ugra in the field of the digital industry and ensuring information security in this regard, yielded following results.

The state program "Information Society of the Khanty-Mansiysk Autonomous Area-Ugra for 2016-2020", adopted and operating in the Khanty-Mansi Autonomous Area-Ugra, defines following as the main directions for development of the sphere of information and communication technologies: normative regulation; personnel education; formation of

research competencies and technical groundwork; information infrastructure; information security.

In Nizhnevartovsk, the adopted “Strategy for the socio-economic development of the city of Nizhnevartovsk until 2030” is approved by the decision of the Duma of the city of Nizhnevartovsk dated May 25, 2018 No. 349, its provisions are aimed at creating a support system for search, applied research in the field of information and communication technologies.

The main goals related to the information infrastructure are defined - this is the development of communication networks of the system of Russian data centers, introduction of digital platforms, as well as creation of an effective system for collecting, processing, storing and providing consumers with relevant and reliable data. Provided information security is aimed at achieving a state of security of the individual, society and state from internal and external information threats.

By resolution of the city administration of Nizhnevartovsk dated 07.25.2018 No. 1053, an Action Plan for the implementation of this Strategy was approved, one of its points (1.5) provides for the improvement of transport services in the city, bringing the quality of urban roads to regulatory requirements, improving road safety; creating a favorable and comfortable living environment for city residents increasing the level of satisfaction of city residents with transport infrastructure by at least 80% by 2030, etc.

In addition, in Nizhnevartovsk, it is planned to implement the large-scale project “Digital Information Model for the Development of the City Territory” (CIM URT). The priority direction of the project is the introduction of a digital information model for development management of Nizhnevartovsk. A project of this magnitude is planned for the first time not only in the Khanty-Mansi Autonomous Area-Ugra, but also in Russia. The project aims to ensure the effective use of the existing infrastructure of the city, the process of managing development of the territory.

As the head of the Department of Architecture and Urban Planning of the city administration, Alexei Rakitsky, explained, “the digital information model for managing the development of the city’s territory is an object-oriented parametric three-dimensional model of the current state and planned development of the city with data on the location, characteristics of terrain objects, connections between them and topographic surface, about terrain objects, about physical, functional and other characteristics. The model was created to solve specific applied problems and make managerial decisions on the development of the territory, including with the participation of residents." Certain elements of the program are gradually being introduced, for example, automated traffic control systems, the Smart Transport application, which allows to track the movement of public transport online, etc.

Thus, in the context of the formation of a full-fledged digital environment, including in the transport sector, the issue of information security of data is not adequately addressed.

Apart from this, Ugra Research Institute of Information Technologies is investigating this issue, which implements the following measures to ensure information security in the Khanty-Mansi Autonomous Area-Ugra: implementation of information security systems in accordance with the requirements of the FSTEC and the Federal Security Service of Russia; certification of personal data information systems, state and municipal information systems; information security audit and information security incident investigation; regulatory and methodological support of information systems in the field of information security; organization and conduction of training courses to ensure information security.

4 Discussion

Debatable is the question of the content of the concept of “information security”. Traditionally, information security is regarded as the ability of the state, society, and

individual: to provide with a certain probability sufficient and secure information resources and information flows to maintain its life and vitality, sustainable functioning and development; to resist information dangers and threats, negative information impacts on the individual and public consciousness and the psyche of people, as well as on computer networks and other technical sources of information; develop personal and group skills and skills of safe behavior; to maintain constant readiness for adequate measures in the information confrontation, no matter who it is imposed by [2]. Information security is considered as a way to ensure the security of the information system and reduce the risks of various kinds of threats associated with its functioning (usually cyberattacks). However, opinions are expressed that this concept cannot be considered as a concept associated only with objects of informatization, quite often such threats are of an "internal nature" and are associated, first of all, with the human factor.

Turning to the annual analytical report in the field of IT - the Solar JSOC Security flash report, allows us to assess reality of the current state of information security in Russia, so in the second half of 2018 the number of attacks aimed at gaining control over the infrastructure increased by 20%, by 37% - the number of attacks aimed at stealing money. In 2018, there were a number of major viral infections of technological networks isolated from the Internet (ACS TP segment). 70% of complex targeted attacks start with phishing. Compared to 2017, the number of DDoS attacks almost doubled - by 95%. Almost half of internal information security incidents are data leaks. So, internal incidents in 2017 exceeded external ones - 50.1% / 47.9%, however, in 2018 the situation changed dramatically - external attacks amounted to 54.2%, while internal ones - 45.8%. The longest attack lasted 280 hours (11 days and 16 hours). Typically, attackers stop malicious activity after 1.5-2 hours. 2018 statistics confirm that the DDoS threat is most relevant for industries whose critical business processes depend on the availability of online services and applications.

Thus, the development of the transport industry using digital technologies requires close attention and adoption of measures aimed at preventing threats and ensuring safety of information data.

5 Conclusion

The imperfection of the regulatory framework governing information security, the lack of effective mechanisms for its implementation - these are the main issues that accompany the process of providing transport services. The paper substantiates the need to build a single coordination system of interaction "state - subject of the federation - municipality - enterprise", as well as the establishment of communication between transport organizations. It seems that it is necessary to build such a system of transport relations that will ensure effective information security in the field of transport services. This system should be based on the relationship "state - subject of the federation - municipal formation - enterprise", be provided with vertical communication of all structural units of this system. However, even a "perfectly" built system is not able to fully provide stable and efficient operation. In this regard, it is necessary to form sustainable links between transport organizations. Therefore, further development of the transport industry will be futile without the realization that in the digital industry the issue of protecting information is the primary task of any subject of relations.

References

1. W. Strielkowski, E. Volkova, L. Pushkareva, and D. Streimikiene, Energies **12(7)**, 1392 (2019).
2. E.B. Belov, V.P. Moose, R.V. Meshcheryakov, A.A. Shelupanov, *Fundamentals of Information Security* (Moscow, Hot line - Telecom, 2006).
3. R. Kolobov , U. Filatova, V. Borshcheniuk, N. Semerianova, D. Bayanov, E3S Web of Conferences **110**, 02095 (2019), DOI: 10.1051/e3sconf/201911002095
4. V.A. Lez'Er, N.A. Semeryanova, A.V. Kopytova, MATEC Web of Conferences **239**, 04027 (2018), DOI: 10.1051/matecconf/201823904027
5. N. Semeryanova, O. Fedorenko, A. Kopytova, MATEC Web of Conferences **239**, 04013 (2018), DOI: 10.1051/matecconf/201823904013
6. E. Vozniak, A. Burgundosova, A. Kopytova, MATEC Web of Conferences **239**, 01016 (2018) DOI: 10.1051/matecconf/201823901016
7. V. Lez'Er, N. Semerianova, A. Kopytova, Y. Truntsevsky, E3S Web of Conferences **110**, 02093 (2019), DOI: 10.1051/e3sconf/201911002093
8. E. Vozniak, T. Slavina, A. Kopytova, MATEC Web of Conferences **193**, 04020 (2018), DOI: 10.1051/matecconf/201819304020
9. D. Izvin, V. Lez'Er, A. Kopytova, MATEC Web of Conferences **170**, 01065 (2018), DOI: 10.1051/matecconf/201817001065
10. Y.V. Truntsevsky, I.I. Lukiny, A.V. Sumachev, A.V. Kopytova, MATEC Web of Conferences **170**, 01067 (2018), DOI: 10.1051/matecconf/201817001067
11. V. Lezier, M. Gusarova, A. Kopytova, IOP Conference Series: Earth and Environmental Science, **90 (1)**, 012069 (2017), DOI: 10.1088/1755-1315/90/1/012069
12. N. Zotkina, M. Gusarova, A. Kopytova, Advances in Intelligent Systems and Computing **692**, 1204-1213 (2018), DOI: 10.1007/978-3-319-70987-1_129
13. U. Filatova, N. Semeryanova, E. Vasilev, E3S Web of Conferences **91**,08064 (2019), DOI: 10.1051/e3sconf/20199108064
14. A. Kopytova, MATEC Web of Conferences **106**, 08056 (2017), DOI: 10.1051/matecconf/201710608056
15. A. Minnullina, A. Mottaeva, IOP Conference Series: Earth and Environmental Science **90**, 012123 (2017), doi:10.1088/1755-1315/90/1/012123
16. N. Zotkina, A. Kopytova, M. Zenkina, O. Zhigunova, MATEC Web of Conferences, **106**, 08058 (2017), DOI: 10.1051/matecconf/201710608058
17. A.V. Kopytova, N.S. Zotkina, I.G. Reshetnikova, MATEC Web of Conferences **239**, 04012 (2018) DOI: 10.1051/matecconf/201823904012
18. N. Zotkina, S. Bardasov, M. Gusarova, A. Kopytova, MATEC Web of Conferences, **106**, 08050 (2017), DOI: 10.1051/matecconf/201710608050
19. I. Skvortsova, R. Latyshev, Y. Truntsevsky, E3S Web of Conferences **110**, 02167 (2019), DOI: 10.1051/e3sconf/201911002167