Technical capabilities and safe use of mobile communications 6G in railway transport

P.A. Plekhanov[1*] and *A.N.* Kartashova[1]

[1] Emperor Alexander I St. Petersburg State Transport University, 190031, 9 Moskovsky pr., Saint Petersburg, Russia

Abstract. The purpose of the study is to describe the technical capabilities and promising approach to the safe use of 6G mobile communications in railway transport. The study used risk management methods in railway transport in accordance with international experience. As a result of the study, information about future 6G networks was systematized, the advantages of their specific technical characteristics over 5G networks were demonstrated, and methods were proposed to ensure the safety and security of information messages transmitted in railway telecommunication networks. In the context of the technical description of 6G networks, the following issues are considered: assessing the quality of services provided (including using indicators of the quality of human physical experience), the use of radio frequencies and combating multipath propagation of signals (based on more advanced methods of multiple access and filtering), the use of more effective modulation and channel coding methods, development of antenna array technology with multiple transmitting and receiving antennas and the use of reconfigurable intelligent surfaces, functional network architecture (based on software-defined networks and network functions virtualization) and its physical implementation (through the construction of a space-terrestrial integrated network), the use of a new internet protocol (covering several levels of interconnection). In the context of ensuring the safety and security of transmitted information messages, the issues of identifying threats and possible countermeasures by implementing additional settings and functions of safety and security 6G networks are considered. The proposed approach allows us to justify the safe use of 6G mobile communications in railway transport.

1 Introduction

Mobile generations replace each other approximately once every ten years. Since the 1980s. five generations of mobile networks have appeared, each of which has increasingly expanded the possibilities for interaction between subscribers. The sixth generation mobile communication networks 6G, which by 2030 should replace the networks of the fifth and previous generations, will make it possible to implement currently unavailable services in the field of infocommunications for individual users and organizations including railways [1-6].

* Corresponding author: pavelplekhanov@gmail.com

The 6G network concept is defined as IMT-2030 (International Mobile Telecommunications) along with the previous 3G network concepts – IMT-2000, 4G – IMT-Advanced and 5G – IMT-2020. 6G networks are discussed in the reports of the International Telecommunication Union – Radiocommunication Sector (ITU-R), releases of the 3rd Generation Partnership Project (3GPP), as well as in studies of the world's largest manufacturers of telecommunications equipment (Huawei, Ericsson, etc.).

Today we can identify the following main services that are not available in 5G networks and are implemented on the basis of 6G networks:

holographic communications – the transmission of three-dimensional images from one or more sources to one or more destinations, which requires a combination of ultra-high data rates and ultra-low signal latency;

tactile Internet applications – transfer of tactile sensations to enable remote actions that require fine motor skills (for example, carrying out remote critical manual manipulations), which requires close to 100% end-to-end network reliability;

multiservice applications of Extended Reality (XR), combining the capabilities of Virtual Reality (VR), Augmented Reality (AR) and Mixed Reality (MR) and requiring ultra-precise positioning;

ultra-high-speed network access anywhere and anytime for a significant number of both mobile and stationary user devices due to large capacity, stable coverage, high connection density and energy efficiency [7, 8].

The purpose of this study is to summarize the available information on the technical capabilities of future 6G networks in comparison with networks of previous generations and to formulate proposals for the safe use of 6G networks in railway transport.

2 Materials and methods

The implementation of promising services in 6G networks is possible based on more advanced technical characteristics compared to previous 5G networks (Table 1).

Table 1. Technical characteristics comparison of 5G and 6G networks

Technical characteristics		5G networks	6G networks
Maximum frequency channel width, GHz		1	100
Spectral efficiency, (bit/s)/Hz	Maximum	30	60
	Custom	0.3	3
Service area throughput, (Gbit/s)/sq. m		0.01	1
Energy efficiency, pJ/bit		undefined	1
Radio interface parameters	Signal delay, ms	1	0.1
	Jitter (time offset of the real signal from the ideal one), μs	undefined	0.1
Data transfer rate, Gbit/s	Maximum	20	1000
	Custom	< 0.1	< 100
Density of user devices, million/sq. km		1	10
Permissible speed of user devices movement, km/h		500	1000
Positioning accuracy, cm		10	1
End-to-end service reliability, %		99.999	99.99999

It is assumed that the signal level in the 6G network at the edge of the service area will be 10 dB higher than in 5G, and the capacity (the number of user devices that can be served,

all other things being equal) will be 1000 times greater. At the same time, for environmental purposes, the average battery life of a 6G network user device is assumed to be 20 years.

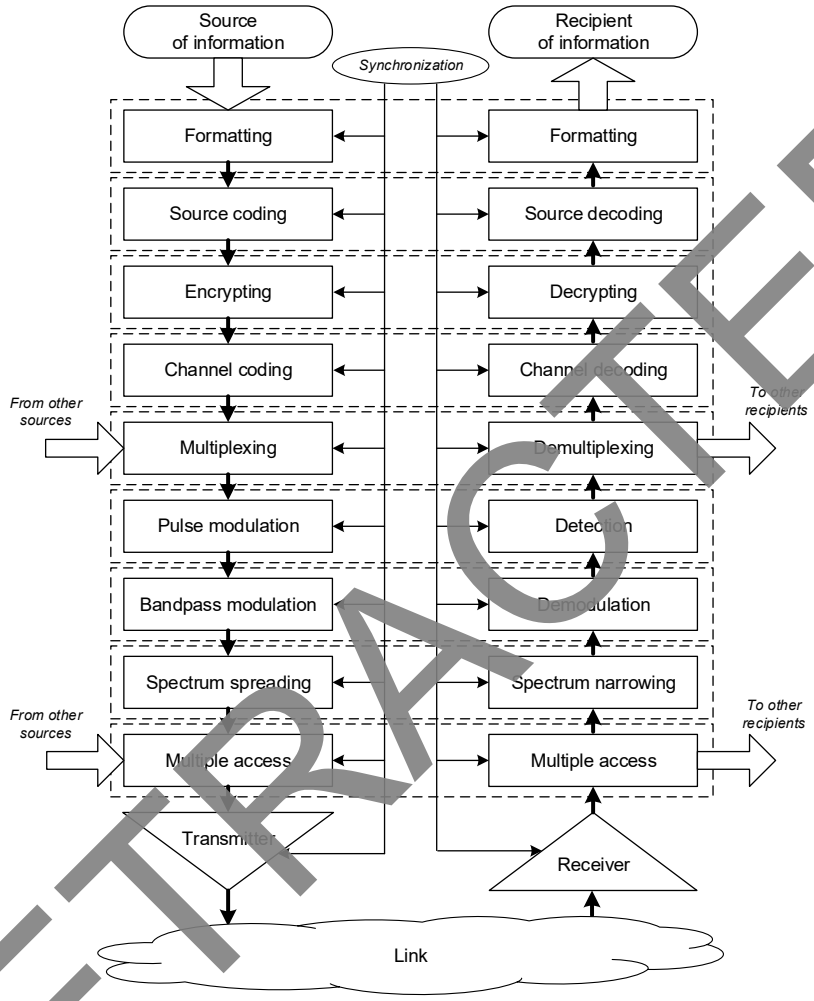

Fig. 1. Complete typical structure of a digital communication system

Basic services (applications):

in 5G networks – eMBB (enhanced Mobile Broadband), mMTC (massive Machine Type Communications), URLLC (Ultra-Reliable Low Latency Communication);

in 6G networks – MBRLLC (Mobile Broadband Reliable Low Latency Communication), mURLLC (massive Ultra-Reliable Low Latency Communication), HCS (Human-Centric Services), MPS (Multi-Purpose Services).

HCS provided in 6G networks should be evaluated not only based on standard Quality of Service (QoS) and Quality of Experience (QoE) metrics, but also using Quality of Physical Experience (QoPE) metrics. QoS indicators include, for example, signal delay and data transfer rate, QoE is the rating given by the user for the service provided, and QoPE is the parameters of a person's physiological reactions (emotions, gestures, etc.) to the service.

Universal MPS of 6G networks include communication, computing, positioning, control, etc. services.

The capabilities of 6G mobile communications can be realized using the terahertz (from 300 GHz to 3 THz) and sub-terahertz (from 100 to 300 GHz) frequency ranges, the use of 6G radio electronics in which is currently under consideration and regulation at the international and national levels.

6G networks involve the use of improved existing and innovative signal conversion and transmission technologies in accordance with typical digital communications system processes (Figure 1).

Existing 4G and 5G networks in the sub-6GHz frequency range face the problem of signal fading due to multipath propagation. To combat this phenomenon and its consequence in the form of intersymbol interference, the Orthogonal Frequency Division Multiple Access (OFDMA) is used, when the transmitted symbol is «split» and transmitted in parts using orthogonally spaced subcarrier frequencies. However, this method is characterized by a significant ratio of the maximum signal power to the average over a certain period of time («peak factor»), which leads to increased energy consumption, in particular of mobile stations. In order to reduce it, the uplink uses the Single-Carrier Frequency Division Multiple Access (SC-FDMA) of frequency division multiple access with a single carrier frequency, which allows signals to be transmitted not simultaneously on subcarrier frequencies, but sequentially. Along with this, the following two methods are effective for 5G and 6G networks:

Filter Bank Multi-Carrier (FBMC), when each subcarrier frequency of the OFDMA signal is filtered separately, which reduces the level of out-of-band emissions and increases the signal's resistance to interference between subcarriers;

Universal Filtered Multi-Carrier (UFMC), in which not each subcarrier frequency is filtered individually, but groups of several neighboring subcarriers, which also leads to a reduction in out-of-band emissions, but without a significant increase in the symbol length and, as a result, without increasing transmission delays.

Also a promising technology is the Non-Orthogonal Multiple Access (NOMA), which assumes that multiple access based on signal power distributions. In this case, each user can be provided with the entire channel capacity during the entire communication session.

In existing 4G and 5G networks, along with various Phase-Shift Keying (PSK) options, standard Quadrature Amplitude Modulation (QAM) schemes are used. The latter is a type of amplitude modulation and is the sum of two modulated (carrier) signals of the same frequency, phase-shifted relative to each other by 90°, while each signal is amplitude modulated by its own modulating (information) signal. For 6G networks, the advanced QAM schemes already tested in 5G are promising:

rotated QAM – standard QAM with phase rotation applied to symbols;

Irregular QAM – the use of various QAM optimization technologies, for example, some variants of Amplitude and Phase-Shift Keying (APSK).

In addition, 6G allows the use of modulation methods such as multidimensional modulation (using more degrees of freedom by increasing the complexity of the signal) and index spatial modulation (transmitting information using indices of transmitting antennas in addition to traditional symbol modulation methods).

The most important issue in wireless communications is the use of efficient channel coding methods. If in 2G networks convolutional codes were used (the code sequence is a convolution of the encoder response to the input information sequence), in 3G and 4G – turbo codes (cascades of parallel connected systematic codes), then for 5G and, in the future, for 6G to ensure high throughput the use of polar codes (based on signal polarization) and Low-Density Parity-Check codes (LDPC), which are based on block linear codes with parity check.

One of the key technologies for 6G networks is MIMO (Multiple Input – Multiple Output) antenna array technology, which first appeared in 3G networks and has become widespread in 4G and 5G, providing a physical implementation of the Space Division Multiple Access (SDMA). If 5G uses «Massive MIMO» technology, when the base station uses antenna arrays containing more than a hundred elements, then in 6G it is planned to use «Ultra-Massive MIMO» with Extremely Large Aperture Arrays (ELAA), consisting of several hundreds of elements that are controlled using artificial intelligence capabilities. In addition, 6G involves the use of Reconfigurable Intelligent Surfaces (RIS), which are two-dimensional planes with software-configurable antenna elements.

The proposed functional architecture of the 6G network, unlike 5G, is much more user-oriented and is built on the principles of Software-Defined Networks (SDN) and Network Functions Virtualization (NFV). It allows each User Equipment (UE) to have its own «virtual instance» of the core network based on a decentralized structure of «virtual instances», which includes Network-layer Service Nodes (NSN) and User-layer Service Nodes (USN) (Figure 2).

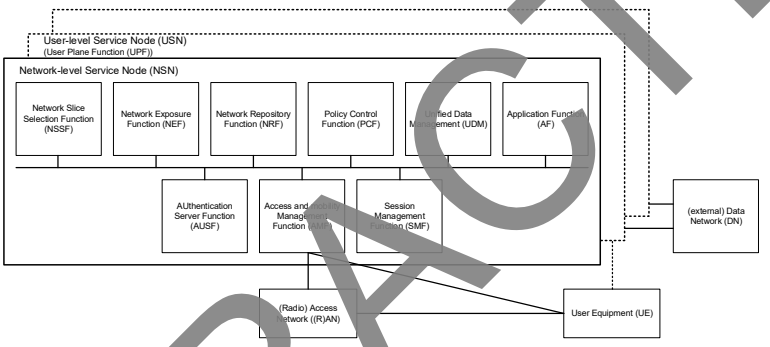

Fig. 2. 6G network proposed functional architecture

Trusted decentralization of the architecture can be implemented based on blockchain technology. At the same time, NSN is the point of primary connection of the UE to the network through the radio access network RAN and is responsible for authentication and identification procedures when registering access. In turn, each of the collection of USNs (which, in accordance with the NFV principle, can be completely distributed and self-organized) belongs to only one UE and implements all the functions of the core network of the user layer and control plane. This approach makes it possible to apply adaptable service policies for each UE, including in the areas of quality and security.

The physical implementation of the 6G networks architecture is assumed to be based on the construction of a Space-Terrestrial Integrated Network (STIN) using, among other things, communication satellites, as well as manned and unmanned aerial vehicles. In this regard, an important innovation in the architecture of 6G networks is the end-to-end use of the New IP protocol instead of the standard IP protocol versions IPv4 and IPv6, since the TCP/IP protocol stack that is used today in Land mobile networks, not suitable for STIN networks. This is due to the low efficiency of using the TCP/IP protocol stack compared to satellite communication protocols due to the presence of relatively large delays in data transmission and a high probability of a bit error.

The New IP protocol is intended to be used not only as a network layer protocol for interaction (like the standard IP protocol), but also to ensure the integration of the functions of the data link and transport layers along with the network layer (Figure 3).

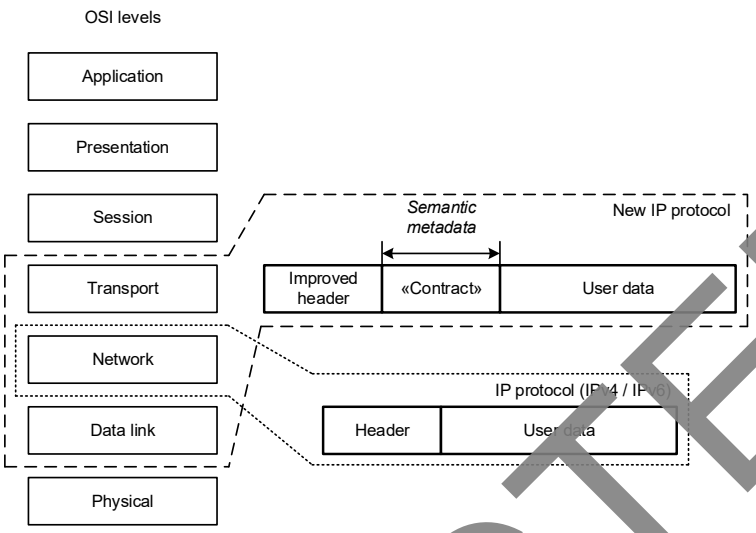

Fig. 3. New IP protocol using

Packets, in accordance with the New IP protocol, will be divided into three components:

Improved header (over IP) to support a wide variety of addressing schemes with different address structures, semantics, and lengths, and to correct security-related issues in existing IP address headers (e.g., unauthenticated source addresses, which expose a variety of attacks);

«Contract» is a new component that allows you to include semantic metadata in packages (for example, directives for processing packages, measurement data of parameters of transmitted packages, etc.), used to establish service level guarantees and simplify service procedures in general;

User data, including allowing applications to structure payloads and differentially process them to facilitate the use of advanced network coding schemes without compromising privacy.

At the same time, one of the critical characteristics of the New IP protocol is its backward compatibility to ensure the ability to work as part of the existing TCP/IP protocol stack.

3 Outcomes

For the deployment of 6G networks the initial task is to identify within the framework of the ITU the specific radio frequency bands. It is assumed that the continuous width of these bands will be at least 1 GHz. Next, it is necessary to conduct an audit of the occupancy of the specified frequency ranges by various radio services, propose ways to ensure electromagnetic compatibility, and also carry out work on the transfer of individual frequency bands for their subsequent use by 6G networks (spectrum conversion). It is also possible to use the possibilities of spectrum sharing – the joint use of the same radio frequency bands by different operators (since the spectrum allocated on an individual basis may be used inefficiently by some operators).

The decisions made need to be consolidated in the appropriate regulatory framework, including issues of sanitary and epidemiological requirements for the placement and operation of 6G radio-electronic equipment and methods for calculating sanitary protection zones.

The use of 6G mobile communications in railway transport, including train automation, must take into account special safety and security requirements [9-13]. It is necessary to ensure the integrity, reliability (authenticity), timeliness and orderliness of transmitted information messages.

To do this, you must first determine the composition of the main and additional functions of 6G systems when organizing technological train and station radio communications networks and wireless data transmission [14, 15], and then carry out a identification of threats associated with the implementation of these functions.

For these purposes, you can use the international standard IEC 62280, which contains requirements for safe and secure data transmission in railway telecommunication networks: for transmitted information messages, characteristic threats may arise as a result of the influence of both the communication network itself and the external environment (physical and anthropogenic) (Table 2).

Table 2. Description of threats to railway data transmission systems.

Typical situations in which the presence of threats is possible	Possible prerequisites for the occurrence of the situation	Possible threats in this situation	Possible causes of threats (dangerous events)
More messages received than were sent	One or more messages are repeated, or an extraneous message is added to the stream	Repeating the message	Systematic failures of hardware (1); systematic failures of software (2); accidental failures of hardware (3); aging of hardware (4); use of uncalibrated (untrusted) tools (5); use of tools for other purposes (6); incorrect replacement of hardware (7); incorrect updating or replacement of software * (8); secret listening of conversations (including using special devices) (9); unacceptable modifications of software tools (10); transmission of unauthorized messages (11)
		Inserting the message	(1) – (11); interference on an adjacent channel (wired or radio) (12); cable switching errors (13); human errors (depending on the specifics of a particular application) (14)
More messages received than were sent	One or more messages are deleted from the stream	Deleting the message	(1) – (10); (12) – (14); physical damage to cables (15); antenna breakdown (16); effects of signal fading (17); electromagnetic interference (18); thermal noise (19); magnetic storms (20); fires (21); earthquakes (22); lightning discharges (23); overloads in the communication network (24); damage or disconnection of hardware (25)
The same number of messages received as were sent	All messages in the stream are correct in content and delivery time, but have the wrong order	Reordering the messages	(1) – (8); (13); (14); (17)
	The delivery time of any stream message exceeds the nominal time interval	The message delay	(1) – (5); (7) – (10); (13) – (15); (17); (20) – (25)

Typical situations in which the presence of threats is possible	Possible prerequisites for the occurrence of the situation	Possible threats in this situation	Possible causes of threats (dangerous events)
	Any message in the stream has been changed (distorted)	Change (distortion) of the message	(1) – (10); (12) – (24)
	The recipient of the message in the stream believes that its sender is different from the expected one	The message substitution	(8); (10) **; (11) **
* this dangerous event in the IEC 62280 standard is not associated with the occurrence of any specific threats, however, practice shows that it can be the cause of all the threats considered ** in this case, the message is fraudulent from the very beginning, therefore it is necessary to have enhanced protection (for example, the use of a key) *NB.* The dangerous event «secret listening of conversations (including using special devices)» does not pose a threat in itself – the consequences of disclosure of the information obtained during listening may be threats, which is the subject of confidentiality requirements for a specific application of the data transmission system.			

As a result, it is necessary to create a set of additional safety and security settings and functions related to the use of 6G systems.

Next, you should conduct a frequency analysis and assess the impact of the threats, assess the levels of risks associated with the threats, and determine risk mitigation measures, including measures to implement additional settings and functions of 6G systems.

4 Discussion/Analysis of the outcomes

The primary risk mitigation measures to transmitted messages should be to ensure their integrity, reliability, timeliness, and orderliness (as discussed previously). The IEC 62280 standard can also be used here, which sets out the necessary protection measures that should be applied to protect against certain threats (Table 3).

Table 3. Description of threat protection measures for railway data transmission systems

Protection activities	Special requirements for protection activities	Threats against which it is advisable to apply protective activities
Sequence number	Required length of the sequence number; initialization of the sequence number; restoring the number after interrupting the message flow	Repeating the message, inserting the message, deleting the message, reordering the messages
Timestamp	The amount of time increment; time increment accuracy; timer dimension; the absolute value of the timer time in the global unified time system; synchronization of timers of various components; the delay between the formation of information and the setting of its timestamp; the delay between checking the timestamp and using the information	Repeating the message, reordering the messages, the message delay
Interval between messages	Permissible maximum delay time; accuracy of the interval between messages	The message delay

Protection activities	Special requirements for protection activities	Threats against which it is advisable to apply protective activities
Identification of transmitting and receiving devices	Uniqueness of identifiers for all subscribers in the data transmission system; matching the size of the identifier to the data field allocated for it	Inserting the message *
Acknowledgment of the received message	There are no special requirements, since the presence of a reverse channel does not in itself provide protection against any identified threat - this channel only allows you to organize such protection at the application level	Inserting the message **, the message substitution **
Message identification procedure	The message identification procedure is an integral part of the application security process, so detailed requirements for it should be defined in the security requirements specifications	Inserting the message **, the message substitution **
Security code	Detection of errors of all predefined types; the specified probability of detecting corrupted messages	Change (distortion) of the message ***
Cryptography methods	Validity of technical issues of the choice of cryptography methods (performance of the cryptographic algorithm, acceptability of the length of the selected key, frequency of key changes, method of physical key storage); validity of organizational issues of the choice of cryptography methods (confidentiality of the creation, storage, distribution and revocation of keys, management of technical operation of equipment, examination of the adequacy of cryptographic methods in terms of countering the risk of malicious impacts on the data transmission system)	Change (distortion) of the message, the message substitution ***
* applicable only for the identifier of the transmitting device; detects insertion only from an invalid source; if unique identifiers cannot be determined due to the fact that the user is unknown, then cryptography methods should be used ** depends on the specifics of a particular application *** the selection and application of security codes and cryptography methods must be carried out in accordance with the following conditions: – the presence or absence of the possibility of unauthorized access control; – the type of cryptographic code used; – the presence or absence of isolation of the secure process of protecting access to the data transmission system from the application secure process		

5 Conclusion

The use of innovations in the field of signal conversion and transmission, full use of the capabilities of artificial intelligence, software configuration and virtualization of network functions make 6G networks a truly new stage in the development of wireless communications.

The capabilities of 6G can be successfully used in railway transport, including solving issues of train automation. The use of 6G capabilities should contribute to the active implementation of innovations in the work of various railway enterprises, making it possible to increase the efficiency of the industry and ensure the necessary level of quality and safety of transportation services.

References

1. Plekhanov, P., Roenkov, D. (2024). *Substantiation of the Safety of Applying Mobile Communication Technologies for Train Automation.* In: Zokirjon ugli, K.S., Muratov,

A., Ignateva, S. (eds) Fundamental and Applied Scientific Research in the Development of Agriculture in the Far East (AFE-2022). AFE 2023. Lecture Notes in Networks and Systems, **vol 733**. Springer, Cham. https://doi.org/10.1007/978-3-031-37978-9_82.

2. Efanov, Dmitry & Mikhailiuta, Evgenii & Khoroshev, Valerii. (2023). Reliability Models for a Safe Train Traffic Control Systems Accounting the Railway Infrastructure States. 266-270. DOI: 10.1109/RusAutoCon58002.2023.10272854.
3. Anatoly Khomonenko, Maad M. Khalil. E3S Web Conf. **383** 01010 (2023). DOI: 10.1051/e3sconf/202338301010.
4. P. V. Polikarpov, N. K. Uvarov, A. D. Khomonenko (2021). Intelligent Transport Systems and Transport Security **(1),** 33-41. doi: 10.24412/1613-0073-2924-33-41.
5. L. Bozhko, A. Liuniakina. E3S Web Conf. **383** 03006 (2023). DOI: 10.1051/e3sconf/202338303006.
6. Ilia Gulyi, Viktoriya Shavurskaya. E3S Web Conf. **383** 01015 (2023). DOI: 10.1051/e3sconf/202338301015.
7. Saharova MA, Prisyazhniuk SP, Kanaev AK, Oparin EV (2020) *Model of the technical diagnostics process and control of the functional subsystem of the telecommunications network.* Wave electronics and its application in information and telecommunication systems (WECONF 2020), pp 1–5. https://doi.org/10.1109/WECONF48837.2020.9131534.
8. Anufrenko AV, Kanaev AK, Saharova MA (2017) *Diagnostics of the transport data network routes with the neural networks.* In: XX IEEE international conference on soft computing and measurements (SCM). https://doi.org/10.1109/SCM.2017.7970546.
9. Efanov, Dmitry & Khoroshev, Valerii & Osadchy, German. (2023). Principles of Safety Signalling and Traffic Control Systems Synthesis on Railways. 634-638. DOI: 10.1109/ICIEAM57311.2023.10139292.
10. Kurbanov, N. V. Yarmova and L. A. Kodirova, *Remote Control and Monitoring of the Unguarded Railway Crossing System,* 2023 International Russian Automation Conference (RusAutoCon), Sochi, Russian Federation, pp. 993-997, doi: 10.1109/RusAutoCon58002.2023.10272764.
11. S. K. Abdishukurovich, Y. N. Valerevna and A. A. Ayderovna, *Organization of video surveillance at railway crossings,* 2021 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2021, pp. 1-5, doi: 10.1109/ICISCT52966.2021.9670092.
12. Markov DS, Nasedkin OA et al (2020) *Method for assessing probabilistic reliability estimation and safety of railway automation systems redundant structures.* In: IEEE East-West design and test symposium, pp 1–6. https://doi.org/10.1109/EWDTS50664.2020.9224925.
13. A.A. Poroshin, A.B. Nikitin, V.V. Shatokhin, A.G. Kotenko. *Diagnostics and monitoring of railway automation and remote control power supply devices.* Proceedings of 2017 IEEE East-West Design and Test Symposium (EWDTS 2017) (2017), pp. 592-597, https://doi.org/10.1109/EWDTS.2017.8110143.
14. Roenkov, D.N., Plekhanov, P.A. (2021). Journal of Physics: Conference Series **2131** (2021), 042096. https://doi.org/10.1088/1742-6596/2131/4/042096.
15. Nikitin A, Manakov A, Kushpil I, Kostrominov A, Osminin A (2020) *On the issue of using digital radio communications of the DMR standard to control the train traffic on Russian railways*. IEEE East-West Des Test Symp. https://doi.org/10.1109/EWDTS50664.2020.9224707.