ABSTRACT
of the dissertation work Sansyzbay Kanibek Muratbekuly on the topic: «Providing information security for railway automation and telemechanics systems», submitted for the degree of doctor of philosophy (PhD) in the specialty 6D070300-Information systems

Relevance of the work. Over the past 10 years, information technology has become an active participant in the activities of many enterprises in the world, increasing their efficiency and optimizing production and management processes. The message of the President of the Republic of Kazakhstan dated January 10, 2018 sets a complex task for the development of traditional basic industries, including logistics, through the widespread introduction of elements of the Fourth industrial revolution. As a result, the Government of the Republic of Kazakhstan was assigned the task of developing a set of measures for technological re – equipment of basic industries until 2025, which initiated the state program «Digital Kazakhstan» (hereinafter-Digital Kazakhstan). According to the Digital Kazakhstan program, to ensure the further growth of the transport and logistics industry, it is necessary to introduce a transport system that would help increase the transit potential by managing vehicles, strengthen transport security by promptly processing information and developing optimal and rational solutions and control actions.

High-quality transport and logistics infrastructure gives a powerful boost to the development of the economy by increasing the connectivity of the territory and reducing the overhead costs of delivering goods to their destination.

Currently, the country is actively working to reform and develop the transport complex of the Republic.

Due to the vast territory and industry differentiation of the Republic of Kazakhstan, railway transport plays a key role in the logistics chain for most large domestic enterprises.

Kazakhstan's location in the center of the Eurasian continent, between the capacious and dynamically developing markets of Europe and South-East Asia, in the future allows domestic railway transport to achieve effective disclosure of high transport and logistics potential.

Thus, the unity of the economic space, the integrity of the state, the defense and security of the country largely depend on the stable and reliable operation of railway transport.

New railway lines provided internal communications between the regions, increased Kazakhstan's export and transit potential. Mega-projects implemented in Kazakhstan over the past 25 years, which were popularly dubbed «Roads of Independence», «Roads of Life and Hope», were the railway lines Aksu – Degelen, Chromtau – Altynsarino, Shar – Ust-Kamenogorsk, Uzen – State Border with Turkmenistan, Zhetygen – Korgas, Zhezkazgan – Beineu, Arkalyk – Shubarkol and Borjakty – Ersai.

At present, there is a stable growth of freight and passenger traffic in the «transport corridors» and suburban areas of large cities. According to experts' forecasts, the demand for transportation of products tends to grow. Meanwhile, the stock of capacity in many parts of the railway is actually exhausted. Therefore, once again, but already in new economic, technological and organizational conditions, the task of identifying rational, in the economic sense, methods to increase the carrying capacity and capacity of the railway network of the Republic of Kazakhstan is urgent.

At present, the network of railroads of JSC «National Company «Kazakhstan temir zholy» for the purpose of its continuous operation transmits significant amounts of responsible confidential information through various systems of data reception and transmission. Responsible information here is understood to be the information used in a discrete system, the distortion of which brings the system into an inoperable state, at which a dangerous distortion of the functioning algorithm occurs. The commands carrying responsible information directly influence functional security of transportation. In addition, high commercial value is the logistic information about the schedule and location of trains. The basis for ensuring the safety of train traffic are systems of railway automation and telemechanics (RATS).

RATS are a set of technical means that provide control and management with the established level of traffic safety of stationary track and mobile objects of railway transport, in which the role and requirements to the information transfer channels are significantly increased. The trend of development of information transfer systems based on foreign and domestic experience indicates that in addition to traditional means, such as rail circuits, it is necessary to use new systems, such as digital radio channels. At the same time the aspects of information security and noise protection of wireless systems are an important factor.

Nowadays it is impossible to increase the efficiency of railway transport operation in the new economic conditions without reliable and safe high-quality communication as the basis for implementation of the newest automated control systems and provision of operative and periodic information necessary for management and control of the transportation process.

In the program of railway transport development in Kazakhstan for the long term introduction of the latest information technology has one of the priority places. Given the qualitative, high-speed and volumetric characteristics of modern info-communication devices will not only solve the problem of providing traditional services of railway communication, train traffic, transportation of goods and passengers, but also will significantly expand their range through the implementation of programs to automate the transportation process, providing monitoring of cargo and other services, the provision of which is currently limited by the technical capabilities of existing communication devices.

As it is known, for information protection in RATS joint application of legislative, organizational and program-technical measures is required. The main stages of ensuring information security in RATS are identification of the main threats to information security, development of its policy, main directions, system of provision and organizational and legal measures, selection and adaptation of information protection technologies.

The purpose of the thesis is to ensure information security of the first developed national train traffic control system KTCS (Kazakhstan Train Control Systems).

The following problems are solved in the dissertation in order to **achieve the set goal**:

- Analysis of the state of existing systems of railway automatics and telemechanics;
- substantiation and research of the base station coverage model for railway trunking communication;
- definition of methods of information protection in the TETRA radio channel of the national KTCS train traffic control system;
- development of the architecture of the National Train Traffic Control System KTCS;
- security analysis of the authentication protocol for terrestrial trunking radio (TETRA) ;
- carrying out experimental studies for the practical application of radio blocking system to ensure information security on the backbone network.

The scientific novelty of the dissertation is determined by the following results:

1. The analysis of the existing systems of railway automatics and telemechanics was carried out.
2. The architecture of the national train control system KTCS was developed for the first time.
3. An algorithm for interaction on the radio channel, which provides information security trains.
4. Proposed a generalized structure of the control system and train traffic safety.

Research methods. The classical methods of algorithm complexity theory, theory of communication and information transfer, theory of reliability of information systems and mathematical modeling were used in solving the tasks set in the scientific work.

Object of study. Object of research are devices of automatics and telemechanics, information transfer and safety of transportation on railway transport.

The subject of the study is authentication and key generation during data transmission via radio channel.

Reliability of the received results of dissertation work is defined by correct use of the chosen mathematical apparatus at the modern level of mathematical rigor, approbation of results of dissertation research at scientific conferences, seminars and their implementation.

Practical value. The results obtained in the dissertation are relevant when comparing the safety standards for data transmission adopted on the railroads of different countries of the world, as well as their analysis with the subsequent proposal for JSC «NC «KTZ» of recommendations necessary to prepare for the replacement of centralization devices with more modern ones, including the tasks that have been solved under the economic agreement «Concept of modernization and production of railway automation and telemechanics systems».

Provisions for protection. The following tasks were solved based on the research results:

- The analysis of the state of existing systems of railway automatics and telemechanics was performed;
- the architecture of the national train control system KTCS was developed for the first time;
- the algorithm of interaction on a radio channel, providing information safety of movement of trains is developed;
- the generalized structure of a control system and safety of movement of trains is offered.

The structure of the dissertation includes an introduction, 4 sections, a conclusion, a list of used sources and annexes.

The introduction provides a rationale for the relevance of the chosen topic of the dissertation. The purpose, object, subject, and tasks of the dissertation are formulated. The results of conducted research are described, their scientific novelty and practical significance are shown. Data on approbation of the main results of the dissertation work are given.

In the first section of the dissertation the analysis of the current state and justification of the need to modernize the SZhat on the main railway network of the Republic of Kazakhstan was performed. It gives the general characteristics of the problem and sets the research tasks.

Most of the existing train traffic control systems, namely, electric centralization, auto-blocking, control centralization were put into operation in 60-70-80s of the twentieth century. The basis of these systems is relay equipment, which requires regular preventive maintenance, leading to an increase in operating costs for components and the maintenance of a significant number of employees engaged in the current maintenance and repair of this equipment.

On the backbone network of the railway of Kazakhstan the devices of railway automatics and telemechanics serve 35 alarm and communication distances. Thus the list of served systems of railway automatics and the telemechanics providing management and the control over movement of trains, traffic safety makes:

- electric centralization systems for control of arrows and signals (EC);
- Train interval control systems (automatic locking (AB), semi-automatic locking (SAB) and radio locking (RB));
- systems of automatic control of crossing alarm system (APS);
- dispatching centralization (DC) and dispatching control systems (DC).

Table 1 shows the main characteristics of RAT system components in the Republic of Kazakhstan.

Table 1 – Current status of the existing RAT system

№	Name of technical means	Ed ed.	The total capacity of the technical means	Capacities put into operation *(After 2000)*	Capacities put into operation *During the period (1980-2000)*	Capacities operated for more than 37 years *(Until 1980)*
1	Automatic blocking	км.	11346	2681,5	5163,92	3501,5
2	Radio blocking	км	1629	1629	-	-
3	Semi-automatic blocking	км.	2825	1327,47	832,62	664,9
4	Electric centralization of EC (including MPC,ROC)	стрелка	15817 (1216)	2076 (1216)	7888	5853
5	Key dependency	стрелка	412	25	146	241
6	Centralized traffic control (including MPDZ)	км.	12057 (7702)	7702 МПДЦ	2435	1920
7	Mountain centralization	стрелка	361	43	208	110

Based on the presented data, the Railways of Kazakhstan with the total length of the railway network of 15.8 thousand km are equipped with: interval control systems for train traffic - auto – blocking AB-11346 km (71.8%), modern radio – blocking systems (SIRDP-E) - 1629 km (11.5%), semi-automatic blocking PAB-2825 km (16.6%). Dispatcher centralization of the DC is equipped-12057 km (76.3%). The electric centralization of stations includes 15,817 arrows (92%).

According to their quality level, the existing STB systems on the Railways of the Republic of Kazakhstan do not meet the modern requirements of integrated automation of the transportation process, hinder the mass introduction of information technologies, do not ensure the introduction of unpopulated technologies for their maintenance, do not always ensure compatibility with mid- and upper-level systems, and do not provide an optimal level of operating costs for their maintenance and repair.

Using the criteria of moral aging, the state of the following SCS systems on stages and stations is evaluated:

EC devices, AB and PUB devices, RC, APS, and DC devices.

The decision to completely replace the STB systems should be applied taking into account one or a combination of factors:

- the system is outdated;

- the volume of installation work, taking into account defective signs (electrical insulation plastic products), is more than 20% of all installation work;

- the cost of replacing worn-out system elements is more than 25% of the cost of modern systems.

The analysis shows that practically operated means of STB, introduced before 1990, have a long service life, a high level of wear, their quality level does not meet the modern requirements of integrated automation of the transportation process, inhibit the mass introduction of information technologies, do not ensure the introduction of low – maintenance technologies (for EC systems – figure 1, for AB systems – figure 2 and for DC systems-figure 3).

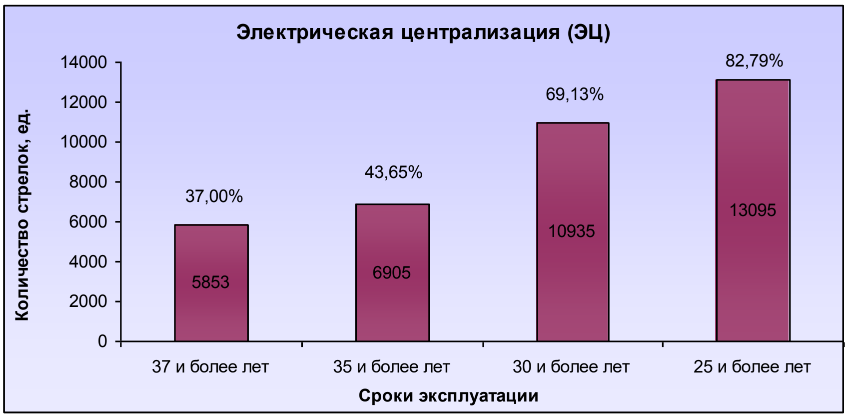


Figure 1-Diagram for the service life of electrical centralization systems

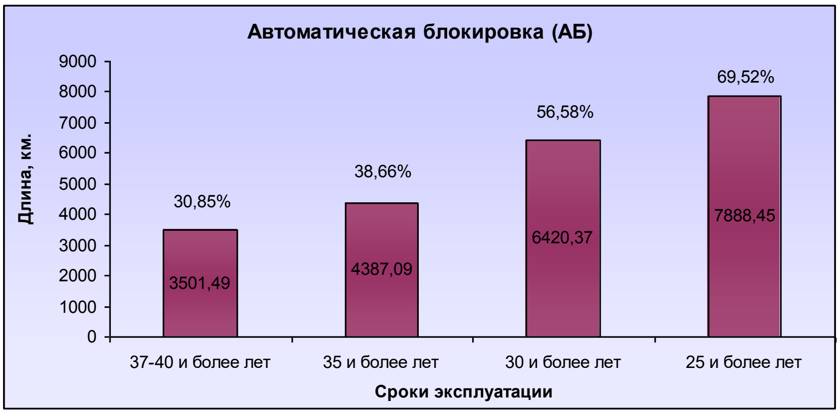


Figure 2-Diagram of the service life of interval train control systems

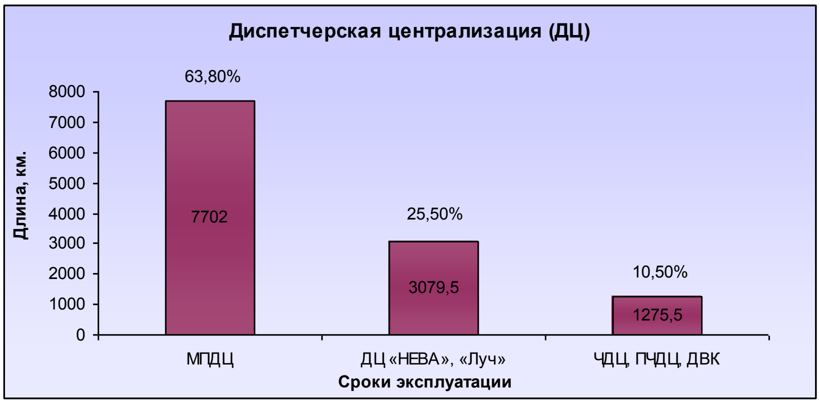


Figure 3 – Diagram of the timing operation of systems of centralized traffic control

The analysis shows that the general state of RAT means is close to critical. More than 70 percent of the main RAT devices that directly provide safety and train control are operated with a long service life. If in the near future measures will not be taken for the reconstruction and modernization of railway sections equipped with existing systems of SFT, by 2025 this figure may exceed 80%.

The large volume of devices with a long service life, the great need to replace the old relay equipment with a new one, the lack of diagnostic tools leads to increased operating costs for their maintenance. The risk of their failure increases every year. The use of relay systems does not allow to provide the modern level of automation of the transportation process, diagnostics and monitoring of automated systems. Absence of normative emergency-repair stock of removed from production a number of relay element base and inability to restore it is a significant factor in the threat of complete shutdown of railway transport activity.

The existing structure and state of the technical means of RAT are a limiting factor in solving problems related to the development of railway transport. Therefore, in recent years, there is a need to introduce modern microprocessor-based RAT systems that most fully meet the tasks of creating an integrated system, as the basis for forming a multi-level security system and a unified automated control system, together with the creation of service centers, remote monitoring and continuous administration of RAT technical facilities.

In addition, the modernization of RATS will have an effect on reducing the turnover of cars, locomotives, reducing the use of shunting locomotives at the station. In passenger traffic will increase the speed of trains on direct sections up to 200 km / h, which in the national scale and will increase the mobility of the population of the Republic of Kazakhstan by providing travel time of no more than 12 hours between the extreme points, which leads to the need to develop a national train traffic control system KTCS.

The second section first developed the architecture of the national train control system KTCS. Based on the application of known security features are achieved the following safety related characteristics: authenticity, integrity, timeliness and consistency of messages. Solved problems of information security and information protection in the system of digital technological radio standard TETRA. The efficiency of the proposed algorithms is shown on the model of architecture of the system protocol TETRA.

During the development of the prototype system "KTCS" pilot tests were carried out at the sites Uzen-Bolashak and Khorgos-Zhetygen, where a multifunctional system was introduced to automate the process of interval control of train traffic in real time using digital radio systems. The effect obtained is characterized by the following:

- a significant reduction in initial capital investments. The full cost of implementation of the first pilot project, including adaptation, testing and construction and installation costs for signalling and communications, is 3.8% lower than the cost of building a traditional AB;

- a significant reduction in construction time (by over 20%);

- substantial reduction of operating costs (reduction of the number of operating personnel by 27% of the number determined by the Project of traditional AB construction, reduction of the total number of vehicles by almost 2 times, reduction of the amount of inspections of signalling devices in accordance with the instruction of TSh-720 by almost 3 times);

- high reliability and availability of the system - "hot standby" of the main elements of the system, when in the event of failure of the main control system goes into a protected state with safe control of occupation and release of the train ferry.

As a result, the KTCS is the most modern command and control system on the railroads and is a communication system that controls and monitors train traffic. The operating principle of the system is explained in Figure 4.

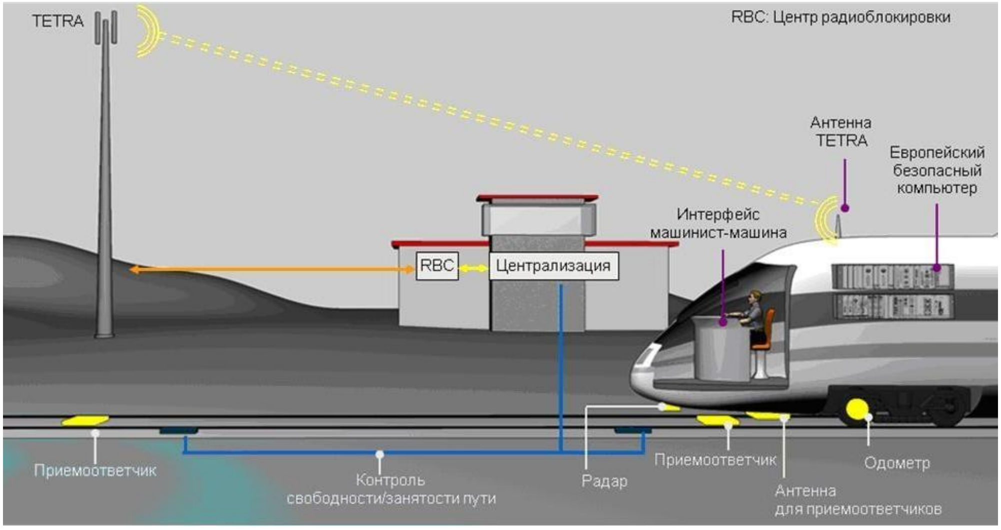


Figure 4 - Working principle of the KTCS system

Figure 5 shows a simplified structure of the MCP on the example of one station. At the upper level of control and monitoring there are automated workstations for the station duty officer, train dispatcher and electromechanics of signalling stations. On the middle level there is a central processor unit integrated with a radio lock center with two sets of RMs, below which there are floor control modules. At the same level, the interface with neighboring centralization units is provided.

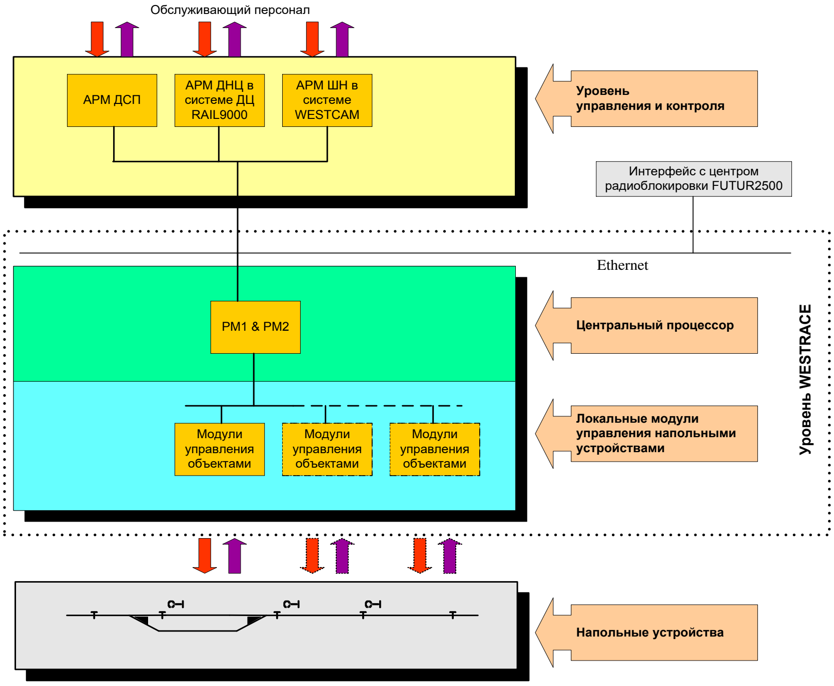


Figure 5 – Structure of MCP on the example of one station

Let's look at an example of data transfer. Stationary device, which uses local radio channel, sends messages to the locomotives located in its area of action in order of priority and receives receipts of notifications from the locomotives about receiving messages. Suppose that the message length of M = 252 bits of content information in the telegram to the locomotive, each additional parcel is encoded by CRC method length N = 48 (detecting ability of which is $3{,}6\text{-}10^{-15}$), is sent to the train on the radio channel at a speed of 900 bits / sec (ie 10800 messages per hour). In this case, the transmission process provides a mechanism for repeating parcels and the corresponding delayed accounting received on board the data for the period of transmission repeats.

A dangerous transmission failure considering repetitions occurs if at the first attempt a transmission error was not detected by checking the control conditions, or the first error was detected and the second was not detected, or the first two were detected and the third was not, etc.

The general efficiency of CRC code application according to CENELEC EN 50159 standard is estimated by the probability of undetected error 2^{-N}, where N-bit code. The common value of the failure stream parameter is 10^{-3}, 10^{-4}, and takes into account the average probability of distortion (not necessarily single) per bit of the transmitted parcel. Hence, the error probability (not necessarily single) in the M+N length parcel is calculated by the formula $(M+N)\cdot 10^{-4}$.

Then the probability of a dangerous failure when transferring the parcel will be:

$$P_{ОП} = 2^{N} P_1 + 2^{-N} P_1^2 + \ldots + 2^{-N} P_1^L = 2^{-N} P_1 \frac{1-P_1^L}{1-P_1} \tag{1}$$

where L=8 is the number of allowed repetitions (according to ICCTT norms); $P_1 = (M+N)\cdot 10^{-4}$ – is the probability that the parcel will not be transferred during the working cycle.

The intensity of a dangerous failure is calculated by a formula:

$$\lambda_{ОП} = 10800 \cdot P_{ОП} = 10800 \cdot 1{,}57 \cdot 10^{-16} = 1{,}7 \cdot 10^{-12}\ 1/ч \tag{2}$$

The method of "cyclic redundant code" reliably detects random changes in data, but is not effective enough in case of unauthorized information change.

The third section is devoted to the analysis of the KTCS multi-level secure data transfer model. Information exchange between KTCS elements is given. Analyzed network architectures GSM-R and TETRA, identified factors affecting the transfer of KTCS in TETRA. The sequence of authentication and key generation during data transmission via radio channel and cryptographic analysis of MAC are proposed.

One of the main requirements on railway transport is safety. Ensuring data protection in control systems is a task that affects the safety of the system. Therefore, data transmitted via radio must be protected from unauthorized influence and distortion.

Based on cryptographic methods, authentication in the Euroradio protocol used by KTCS is implemented. The Euroradio protocol uses a block cipher based method called CBC-MAC as a MAC function. The basic idea of the CBC-MAC algorithm is to encrypt the m message with a block cipher block chaining (CBC - cipher block chaining) and to discard all blocks of cipher text except the last one. For a message consisting of blocks P_1,..., P_k, the MAC value is calculated based on the following formulas:

$$H_0 = 0; \quad H_i = E_k(P_i \oplus H_{i-1}) \quad MAC = H_k. \tag{3}$$

When a session is established at the time of connection, the authentication procedure shown in Figure 6 takes place.

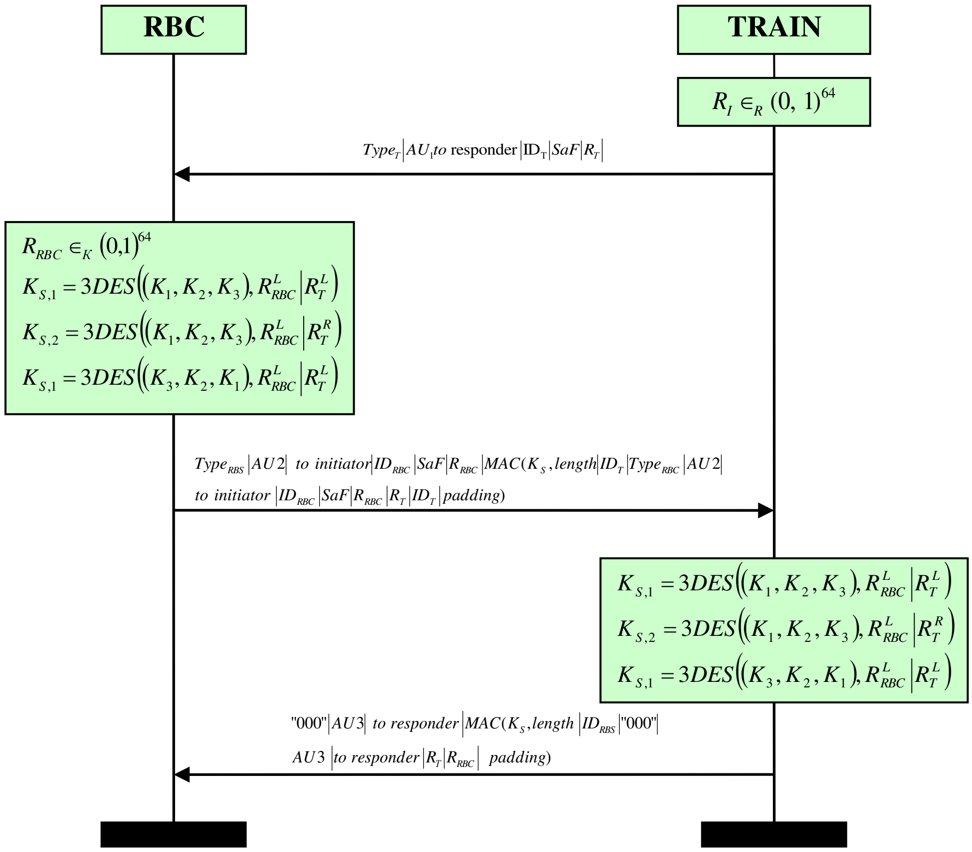


Figure 6 – Authentication and key generation sequence

Party B sends a random number Rb length 64 bits, which is generated by B. Number Rb is stored on the side of B. After receiving this message, party A generates a random number Ra length 64 bits and calculates the MAC in the Text3 field, random numbers Ra and Rb, DA identifier and filling bits. MAC (message authentication code), which is a number that prevents an attacker to counterfeit messages. In fact, the message authentication code (MAC) is a function that takes two arguments (a fixed length K key and an arbitrary length m message) and gives a fixed length value.

To calculate MAC, the Ks session key is calculated based on the Ra, Rb parameters and the Kab authentication key according to the following procedure:

- numbers Ra, Rb are divided into 32 bit blocks.

$$R_A = R_A^L \big| R_A^R \qquad (4)$$
$$R_B = R_B^L \big| R_B^R$$

Three 64-bit keys Ks1, Ks2, Ks3 are calculated by formulae:

$$K_{s1} = MAC\left(R_A^L \middle| R_B^L, K_{AB}\right) = DES\left(K_3, DES^{-1}\left(K_2, DES\left(K_1, R_A^L \middle| R_B^L\right)\right)\right) \qquad (5)$$
$$K_{s2} = MAC\left(R_A^R \middle| R_B^R, K_{AB}\right) = DES\left(K_3, DES^{-1}\left(K_2, DES\left(K_1, R_A^R \middle| R_B^R\right)\right)\right)$$
$$K_{s3} = MAC\left(R_A^L \middle| R_B^L, K'_{AB}\right) = DES\left(K_1, DES^{-1}\left(K_2, DES\left(K_3, R_A^L \middle| R_B^L\right)\right)\right)$$

where $KMAC = (K_1, K_2, K_3)$.

MAC calculation in Euroradio protocol is based on the TripleDES encryption standard, which is a symmetric block cipher. When designing the protocol for the needs of JSC "National Company" Kazakhstan Temir Zholy "is expected to replace TripleDES on the standard of symmetric encryption GOST 28147-89" Information processing systems. The protection is cryptographic. Algorithm of cryptographic transformation".

In KTCS system protection of transferred data is carried out by Euroradio protocol intended for transfer of data connected with safety, on a radio channel with use of open communication networks.

The fourth section contains a description of the developed system and model of radio blocking. The model of covering the base station for railway trunking communication was developed. By experiment, determined the percentage of packet loss in the radio network, losses on the track and Doppler shift depending on the location at a frequency of 450 MHz.

The practical application of the radio blocking system was considered at the section Zhetygen - Altynkol of the Almaty branch of the trunk network. At practical application the questions of communication of the center of radio blocking and the center of switching TETRA, coordination of the center of radio blocking with systems of electric centralization, modernization of the onboard equipment of a locomotive, check of algorithms of work of the onboard and stationary equipment are considered.

At the first stage, the experiments are conducted according to the scheme shown in Figure 7.

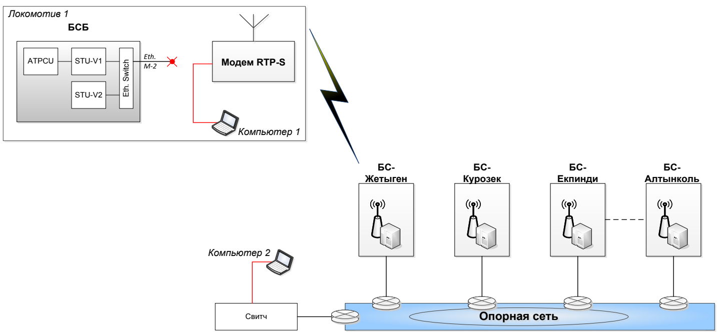


Figure 7 – Scheme of experiments - stage 1

The results of the measurements, which include data on the channel capacity, time of the packets passing, data on the packet loss in TETRA radio network are presented in Figures 8-10.

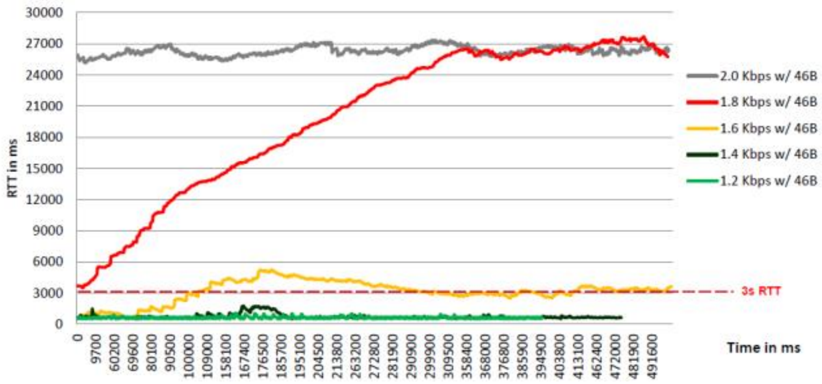


Figure 8 – Passage time of a 46-byte package

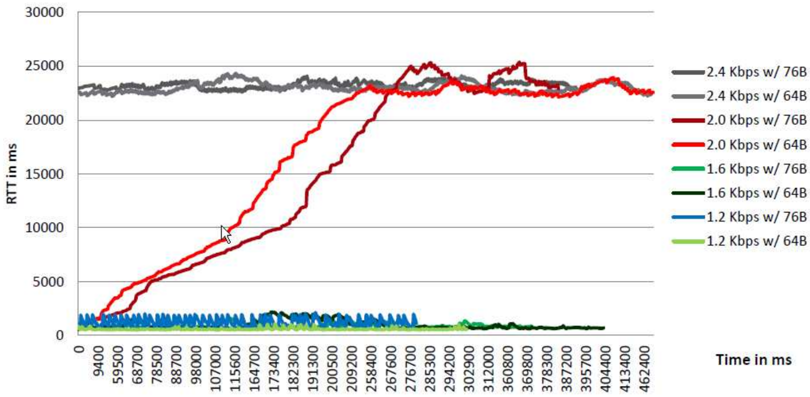


Figure 9 – Passage time of a 64-byte and 76-byte package

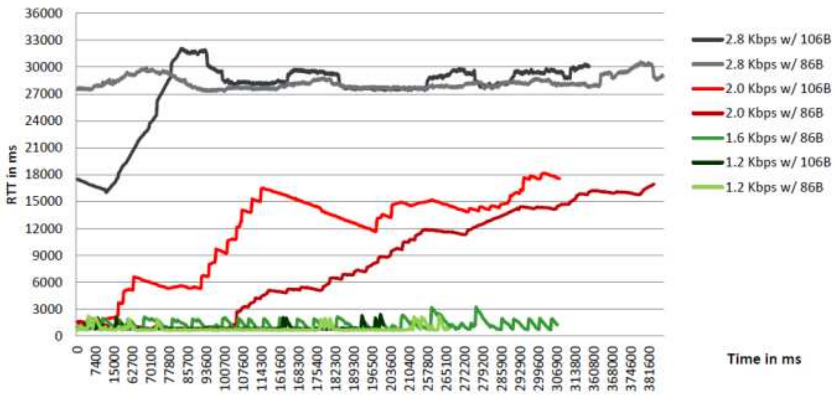


Figure 10 – Passage time of the package of 86 and 106 bytes

At the second stage, the experiments are conducted according to the scheme shown in Figure 11.

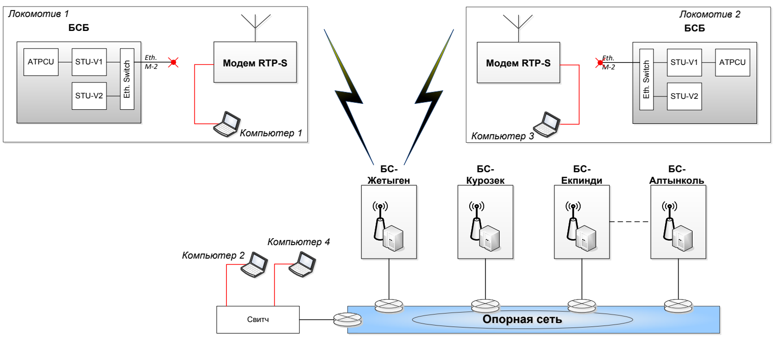


Figure 11 – Scheme of experiments - stage 2

The results of the measurements, including data on the channel capacity, time of the packets passing, data on the packet loss in the TETRA radio network are presented in Figure 12.

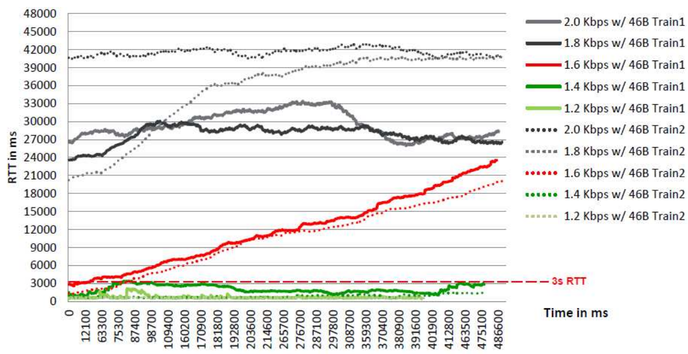


Figure 12 – Time of passage of a package of 46 bytes

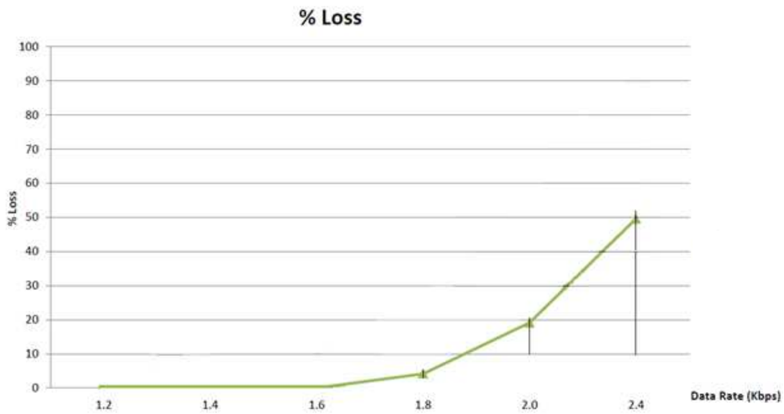


Figure 13 – Percentage of packet loss on the radio network

The experiments show that at any packet size in the TETRA digital radio system, the time of packet passage increases as the load on the system increases. For transmission speeds up to 1.4 kbps the system meets the requirements for packet passing time. Starting from the load of 1.6-2.0 kbps the time of packet passing becomes unacceptably large and reaches 30-40 seconds, which does not meet the requirements. At the same time, the percentage of lost packets (up to 50%) is increasing, with several consecutive packet losses.

The developed model of BC coverage for trunk communication is shown in Figure 14. The base stations are located along the railway with a spacing of 2R, which represents the service distance of one BS. The train is moving at a constant speed along the rail.

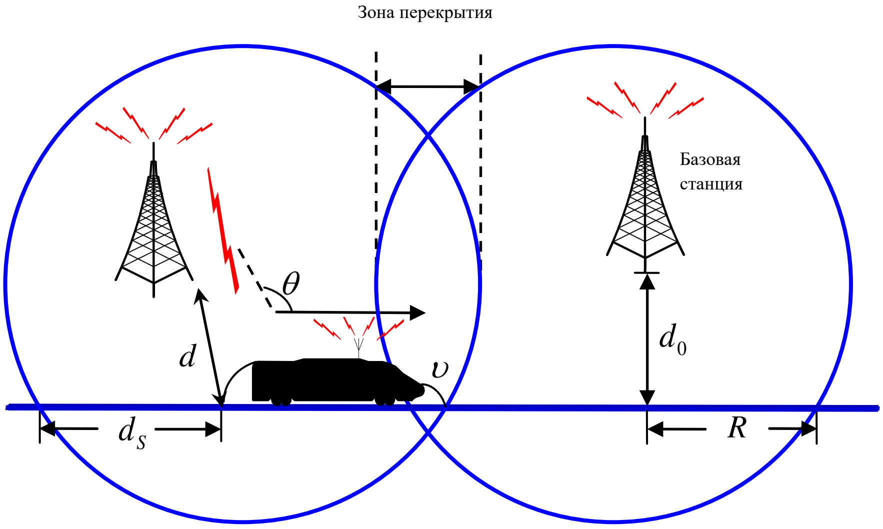


Figure 14 – Coverage model of the base station for railway trunk communication

When the train is in position d_s of the current cell for $0 \leq d_s \leq 2R$, the distance between the BS and the train is $d = \sqrt{d_0^2 + (d_s - R)^2}$, , where d_0 – the distance between the BS and the railway line. Based on the assumption of ignoring the difference in height between the BS antenna and the railway line, the losses when passing the line of sight in the free space is determined:

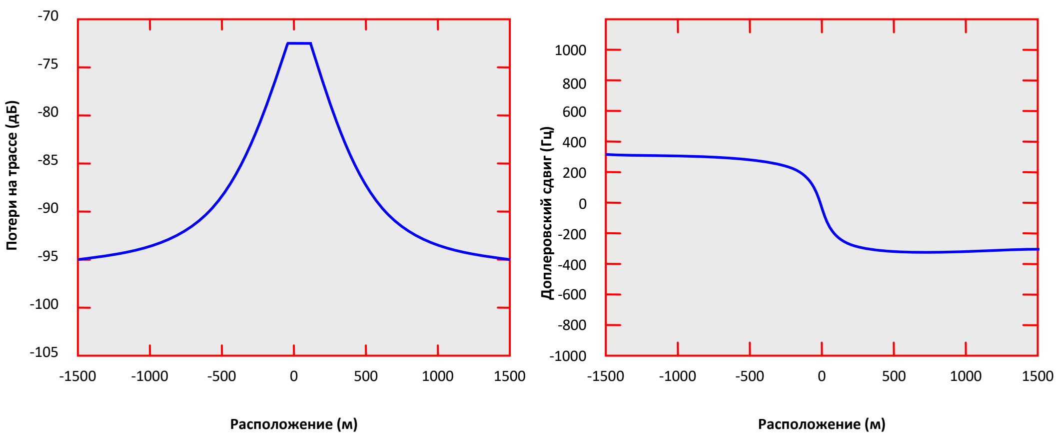
$$L = 20\log_{10}\left[\frac{4\pi df}{c}\right], \quad (6)$$

where f and c - the emitted frequency and speed of light, respectively.

It can be seen from (6) that losses on the L trace are related to distance d and frequency f .

To conduct the experiment, the base station is located at point 0, the radius of cell R is 1500 m, and the speed of the train v is 100 km / h.

Figure 15(a) shows the effect of distance and frequency from losses on the track. As can be seen from the figure losses on the track quickly change depending on the location of the train. When a train moves to the edge of a cell, the losses on the track become more and the corresponding channel state deteriorates. On the contrary, when a train moves to the center of a cell, the losses on the track become less and the corresponding channel state changes better. Thus, periodic change of the channel state causes that power control over time has a great impact on transmission performance.



(а) (б)

Figure 15 – Loss on track and Doppler shift depending on location at 450 MHz

High mobility causes a large Doppler shift and spread. In this section, the ratio of energy in the line-of-sight path to energy in multi-beam propagation is relatively high, and the delay of multi-beam propagation is relatively small. As shown in Figure 14, when a train moves along the rail, the Doppler shift can be calculated as follows

$$f_p = f_d \times \cos\theta, \tag{7}$$

where $f_d = \frac{v}{c} \cdot f$ - maximum Doppler frequency, θ - angle between the direct direction of the train and the line of sight from the BS to the train. Based on the information on geometry, from Figure 14, we have $\cos\theta = \frac{R - d_s}{d}, \quad 0 \le d_s \le 2R.$

Thus, when the BS is located far from the rail, that is $d_0 >> R$, f_p, relatively low, because it will be approximately 90◦. However, this will lead to high losses on the track according to equation (6). Thus, there is a trade-off between loss on a trace and Doppler shift in optimization of BS assignments.

Figure 15(b) shows the Doppler offset along the rail for the carrier frequency of 450 MHz:

- f_p varies in time from the maximum positive value to the maximum negative value when the train moves through a cell;
- there is a Doppler offset while the train is moving;
- f_p although very little when the train moves through the BS, it will encounter a fast Doppler junction;
- f_p will move from the maximum negative value to the maximum positive value when the train moves to the area of overlap between adjacent cells, as shown in Figure 14.

For wireless trunking, serious problems with Doppler shift and fast Doppler transition must be solved before practical application. Serious Doppler shift can lead to difficulties in synchronization and bit error rate. It should be noted that although the Doppler shift is large, its change is so small that it can be accurately estimated and easily compensated for with accurate information about the speed and location of the train. Also, a fast Doppler shift in the center of the cell makes it much more difficult to estimate the channel and the Doppler shift.

The main results and conclusions of the dissertation are presented in the conclusion.

The validity of scientific provisions, conclusions and recommendations put forward for protection is confirmed by the correctness of mathematical apparatus use, correct setting of experiments and their processing; qualitative and quantitative correspondence of theoretical research results and experimental data; practical application of research results.

Probation of work. The main provisions of the dissertation work were reported and discussed:

- XLI International Scientific and Practical Conference "Innovative technologies in transport: education, science, practice" (Kazakhstan, Almaty, KazATK named after Tynyshbaev, 2017),
- International Scientific and Practical Conference "Auezov Readings - 15: The Third Modernization of Kazakhstan - New Concept and Modern Solutions" dedicated to the 120th anniversary of Mukhtar Omarhanovich Auezov (Kazakhstan, Shymkent SKSU named after M.Auezov, 2017);
- V International Scientific and Practical Conference "Intellectual Information and Communication Technologies - a means of implementing the third industrial revolution in the light of the Strategy "Kazakhstan-2030" (Kazakhstan, Nur-Sultan L.N. Gumilev ENU, 2018);
- round table at Hyukshin Co., Ltd. (South Korea, Seoul), June 2018;
- V International Conference "Digital Technology in Science and Industry - 2019" (DTSI-2019), dedicated to the 10th anniversary of the International Information Technology University. (Kazakhstan, MIT, 2019);
- All-Russian Scientific and Technical Conference with International Participation "Efficiency and Safety of Electrical Complexes and Automation and Telemechanics Systems on Railway Transport" (Russia, Omsk State University of Railway Transport, 2019).

Totally, the reports were made at seminars, conferences of different levels and round tables.

Publications. Based on the materials of the dissertation 13 articles, 5 works in the publications included in the list of the CCSON MES RK, 7 works in the materials of conferences, symposiums, seminars, 1 article in the journal included in the Scopus database were published.

Scientific publications:

1. Bakhtiyarova E.A., Sansyzbay K.M. On the development of an interstate standard for axle counting systems // Bulletin of KazATK, «Special issue dedicated to the meeting of the Interstate Technical Committee for Standardization No. 524 «Railway Transport», Astana - 2016, pp. 57-60.

2. Kuandykov A.A, Sansyzbay K.M. Trends and principles of development of world-class railway automation and telemechanics systems // Materials of the XLI International scientific-practical conference on the topic «Innovative

technologies in transport: education, science, practice» Almaty, April 3-4, 2017. p. 11-16.

3. Bakhtiyarova E.A., Chigambaev T.O., Sansyzbay K.M. The technology of the future distributed acoustic sounding DAS in real time // Proceedings of the XLI International Scientific and Practical Conference on the topic «Innovative technologies in transport: education, science, practice» Almaty, April 3-4, 2017, pp. 49-54.

4. Kuandykov A.A., Sansyzbay K.M. The development of the national microprocessor system «KTCS» // Proceedings of the international scientific-practical conference «Auezov readings - 15: The third modernization of Kazakhstan - New concepts and modern solutions», dedicated to the 120th anniversary of Mukhtar Omarkhanovich Auezov. Shymkent, April 13-14, 2017, pp. 276-279.

5. Kuandykov A.A, Sansyzbay K.M Ensuring information security of train traffic through the introduction of the national system «Kazakhstan Train Control Systems» in the railway networks of the country // Proceedings of the V International scientific-practical conference «Intellectual information and communication technologies - the means of the third revolution of the 20th industry of Kazakhstan» Astana ENU, February 22, 2018. C. 460-463.

6. Bakhtiyarova E.A., Sansyzbay K.M. Comparative analysis of microprocessor centralization of arrows and signals // Bulletin of the L.N. Eurasian National University. Gumilyov, Astana 2018, No. 2 (123). S. 30-36.

7. Bakhtiyarova E.A., Kuandykov A.A., Sansyzbay K.M. Standardization and certification of automation and telemechanics systems on the railways of the world and in the Republic of Kazakhstan // Bulletin of KazATK, Almaty 2018, No. 4 (107), pp. 337-346.

8. Bakhtiyarova E.A., Sansyzbay K.M. Risk analysis in case of non-implementation of modernization of TAT systems in JSC «NC «KTZ» // Materials of the XLIII International scientific and practical conference «Innovative technologies in transport: education, science, practice», dedicated to the 140th anniversary of Mukhamedzhan Tynyshpayev. Volume 1, April 17, 2019, Pp. 120-124.

9. Kuandykov A.A, Sansyzbay K.M. Methods of information security protection in railway automation and telemechanics systems // Bulletin of the British Technical University of Kazakhstan, Almaty 2019, № 16, p. 353-359.

10. Bakhtiyarova E.A., Sansyzbay K.M. Risk analysis in case of failure to modernize existing systems in the Republic of Kazakhstan // Materials of the All-Russian scientific and technical conference with international participation «Efficiency and safety of electrical complexes and systems of automation and telemechanics in railway transport», Omsk State University of Railway Engineering, November 28, 2019. S. 97-105.

11. Sansyzbay K.M., Kuandykov A.A., Bakhtiyarova Ye.A., Vlasenko S.V., Mamyrbaev O.Zh. Radio communication channel interaction method, maintaining train performance information security // Journal of Theoretical and Applied Information Technology. 31st March 2020. Vol.98. No 06. pp. 957-969.

12. Bakhtiyarova E.A., Duysebekova K.S., Chigambaev T.O., Sansyzbay K.M. Practical application of the radio blocking system to ensure information security on the backbone network // Industrial transport of Kazakhstan, Almaty 2020, No. 1 P.111-117.

13. Kuandykov A.A., Sansyzbay K.M. The method of interaction over the radio channel, providing information security of train traffic // Program of the XLIV International Scientific and Practical Conference of KazATK named after M. Tynyshpayeva «Innovative technologies in transport: education, science, practice», Almaty 2020, pp. 56-59.

Implementation acts:

1. Information on the implementation of the results of scientific developments in the Hyukshin company (South Korea, Seoul, 2020);

2. The act of implementation of the results of dissertation work in the Branch of JSC «NC «KTZ»-«Directorate of Automation and Digitalization», 2020.