The Basis for Building Integrity Monitoring System of Critical Information in ALS Based on Broadcast Radio Channel

Boris F. Bezrodnyi
Cybersecurity Center
NIIAS, JSC
Moscow, Russia
b.bezrodnyi@vniias.ru

Alexander M. Korotin
Cybersecurity Center
NIIAS, JSC
Moscow, Russia
a.korotin@vniias.ru

Abstract*—The transition to the use of a radio channel for critical information transfer in automatic locomotive signaling (ALS) systems complicates the safety of railway traffic, because in this case it becomes possible to implement computer attacks from the outside of the controlled area that can lead to traffic accidents. Integrity monitoring systems (IMS), ensuring that the received critical information is up-to-date and sent by a legitimate traffic participant, today exist only for ALS systems based on point-to-point data transfer method. That's why the task of constructing IMS for ALS based on broadcast radio channel is actual. The main problems that need to be solved during the building of IMS are considered in this article. The conditions that influence on the choice of security mechanisms in the IMS and the development of updating procedure for security parameters of the integrity monitoring system are determined. It is concluded that the construction of a unified IMS, the use of which would be possible for protection of any ALS based on a broadcast radio channel, seems to be a difficult task. Hence further research in this field should be related to the development of a technique for constructing integrity monitoring systems applicable in ALS based on broadcast radio channel.

***Keywords*— information security; transport security; cybersecurity; safety of railway traffic; automatic train signalling; automatic locomotive signaling system; broadcast radio channel; integrity monitoring system; critical information**

I. INTRODUCTION

Automated control systems are widely used in the field of railway transport to solve problems associated with the control of the transportation process, including, among others, the tasks of ensuring the safety of traffic and the exploitation of railway transport [1, 2]. One of the control systems used to ensure traffic safety at stations and hauls is the automatic locomotive signaling system (ALS), a system for transmitting information about the permissible speed and additional conditions for following the railway rolling stock: permission for movement, speed limit, the route of movement along the railway station to the on-board locomotive devices[1] [3, 4].

The information transmitted by the ALS system in the field of ensuring the safety of the railway transport is attributed to the critical information, i.e. information, the distortion of which translates the system into a dangerous state[2].

The use of radio communication systems in the ALS for transmission of critical information allows to increase the amount of data transferred between the station part and the onboard part of the system and to reduce the likelihood of their distortion [5]. However, such a transition to the use of ALS based on radio channel (ALSR) complicates the ensuring of traffic safety, because in this case the communication channel between the station part and onboard part goes beyond the control zone. There is the possibility of implementing threats to the security of critical information from the side of the external violator, associated with its modification and / or substitution, which can lead to the occurrence of transport incidents. As a protection against these threats, integrity monitoring systems (IMS) can be used to guarantee that the received critical information is up-to-date and sent by the legitimate station or on-board part of the system [6, 7, 8, 9].

Given the fact that the use of an existing solution for protection of critical information is not always possible for ALS systems using the broadcast method of data transfer [10], the problem of constructing integrity monitoring systems for this class of ALS is topical. In this article, the problems that need to be solved during the constructing of IMS for ALS systems based on a broadcast radio channel (ALS-BR) are determined and considered.

II. DEFINITION OF TASKS REQUIRING SOLUTIONS DURING THE CONSTRUCTION OF IMS

Let's consider a railway section equipped with an ALS system based on a broadcast radio channel (see Figure 1). The station part of the system for transmission of sensitive information to the radio channel must first obtain data about the current train situation and the state of the field devices from the systems of determining the free path and the location of the train (SDFPLT), monitoring stations and distances. As a broadcast transmission method is used, the station part sends a message to the radio channel, intended for all traffic participants at the

[1] GOST R 53431-2009. *Railway automation and telemechanics. Terms and definitions.*

[2] OST 32.17-92. *Railway automation and telemechanics safety. Basic concepts. Terms and Definitions.*

section at once. At the same time, the radio communication system used in ALS-BR should have a coverage area sufficient for data transmission to any participant of the traffic, regardless of its location at the section. The onboard parts of ALS-BR installed on locomotives process the received messages and use critical information to ensure the safety of the rolling stock traffic. If two-way exchange between the station part and onboard part of ALS-BR is required to ensure traffic safety at the section, the on-board parts of the system in turn also send messages with critical information, that are further processed by the station part, to the radio channel. As the length of section increases, the coverage of the station part of ALS-BR increases. This means that the station part of the system should receive information about the current train situation at additional stations and hauls and transmit relevant critical information throughout the section. If for some reason this is impossible, for example, there is not enough coverage of the radio communication system or the principle of system decentralization is used, then additional station parts should be installed at the section. Thus, ALS-BR at the section can have several station parts. In this case, the station parts are unified and have the same software and hardware. The onboard parts are also unified.

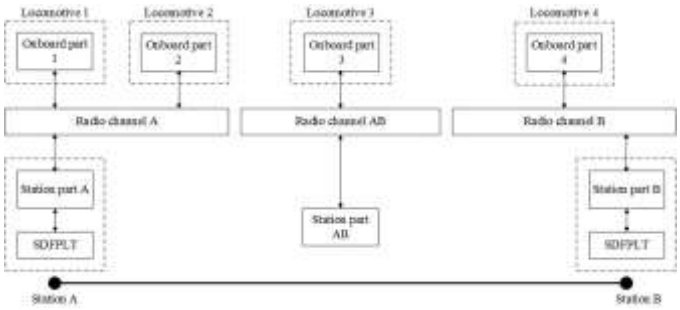

Fig. 1. Structural scheme of ALS based on broadcast radio channel

The violation of traffic safety and the occurrence of traffic accidents at the considered railway section are possible through the implementation of the following security threats of the critical information [11]:

- Sending fake critical information to the radio channel;
- Substitution of the base and/or subscriber station;
- Resending of previously intercepted critical information in the radio channel.

In the course of the research protection mechanisms against these threats were identified. When ALS-BR is used these mechanisms should be implemented in the IMS for traffic safety.

To protect against the first threat, each message of critical information should contain verification information that guarantees the authenticity of the transmitted data, that they were not unauthorized modified during the transmission. The digital signature (DS) or authentication codes (AC) can be used as verification information [12, 13]. To denote the sequence of bits necessary for calculating and verifying DS and AC, within the framework of the IMS, the term integrity monitoring parameter of the critical information is used. At the time of critical information exchange, the integrity monitoring parameters must be located at the station and onboard parts of the ALS-BR and used to calculate and verify the DS or AC. In this case, confidentiality of the integrity monitoring parameters necessary for computing the verification information must be ensured. Thus, if the intruder does not know the integrity monitoring parameters of critical information necessary to calculate the DS or AC, then he will not be able to implement the threat of sending fake information to the radio channel.

To determine the possible mechanisms of protection against the threat of substitution of radio stations, we'll consider a railway section equipped with an ALS-BR system, along which the locomotive L1 is moving. Further during analyzing this threat, for abbreviation, we'll consider under the onboard part of the ALS-BR system only the appropriate on-board equipment of the locomotive L1. Let's suppose that at the moment of time t_0 the onboard part of the ALS-BR establishes a connection with the station part of the system and the exchange of critical information begins between them. At time t_1, the locomotive L1 finishes the traffic on the considered section and the exchange of the critical information between it and the station equipment terminates. Then in order to neutralize the threat of sending fake information at any time $t \in (t_0,t_1]$, the integrity monitoring parameters must be in the station part and onboard part of the ALS-BR. We introduce the function $f(t):[t_0,t_1]\rightarrow\{0,1\}$, which shows the presence of integrity monitoring parameters in the station and onboard parts of ALS-BR as a function of time t. $f(t)=1$, if the station and onboard parts of the ALS-BR have all necessary integrity monitoring parameters to ensure safe exchange of critical information, otherwise $f(t)=0$. Then, $\forall$ $t \in (t_0,t_1]$ $f(t)=1$, $f(t_0)=1$ or $f(t_0)=0$. If the substitution of the radio station occurs at time t, such that $f(t)=1$, then as a protection mechanism, verification information (DS or AC) can be used to ensure the integrity of application-level messages, including critical information, as well as the authenticity of traffic participants, because only legitimate traffic participants know the parameters of integrity monitoring. Thus, if the intruder does not know integrity monitoring parameters of critical information, then the substitution of radio stations will not allow him to impersonate a legitimate traffic participant, and as a result, the implementation of this threat will not violate the safety of traffic. If the substitution occurs at the time t such that $f(t)=0$, which is possible only at the moment of establishing a connection between the station and the onboard parts ($t=t_0$), then the authentication procedure of the traffic participants which allows to determine the authenticity of participants and to transmit to them authenticity of participants should be used as a protection mechanism.

Thus, it is enough to use DS and/or AC to protect against the threat of radio stations substitution during the exchange of critical information between parts of ALS-BR. To protect from the threat of radio station substitution during establishing a connection between ALS-BR parts, if they lack the integrity monitoring parameters necessary for the safe exchange of critical information, it is required to develop an authenticating procedure for traffic participants, which ensures the safe delivery of these parameters.

Timestamps or the sequence number of application-level messages containing critical information may be applied to

block the threat of resending previously intercepted critical information [14, 15].

Building IMS with the use of integrity monitoring parameters leads to the need of solution of the problem of managing these parameters [16]. One of the key management issues is the development of a procedure for updating parameters [17], within which it is necessary to determine the order of performed actions, to select communication channels for data transmission, and to ensure the security of delivery.

Thus, as a result of the research, it was found that during building a IMS, it is necessary to define a mechanism for protection against the threat of sending fake information (DS or AC), to develop an authentication procedure, to choose a mechanism to protect against the threat of retransmission of information, and to develop a procedure for updating integrity monitoring parameters.

III. CONDITIONS AFFECTING THE SELECTION OF PROTECTION MECHANISMS IN THE IMS

As a result of the analysis of sending false information threat and possible protection mechanisms against it, the conditions influencing the choice of DS and AC for the protection of station and onboard messages, presented in Tables 1 and 2 respectively, were determined. The parameter $Trusted_L \in \{0,1\}$ determines the power of attorney of onboard parts of the ALS-BR; I^S_{sec1}/I^L_{sec1} is the maximum amount of information that can be contained in the DS and/or AC to protect station/onboard messages; L_{DS} is the size of the DS for the selected cryptographic algorithm; T^S_{msg}/T^L_{msg} is permissible time of calculation and verification of DS and/or AC for protection of station/onboard messages; T_{DS} is the time of calculation and verification of the DS for the selected cryptographic algorithm; $UA_L \in \{0,1\}$ is the urgency of unauthorized access (UA) threat to the onboard side of the ALS-BR and the compromise of the integrity monitoring parameters stored in it.

TABLE I. CONDITIONS FOR DETERMINING THE POSSIBLE USE OF DS AND AC WITHIN THE FRAMEWORK OF THE IMS FOR STATION MESSAGES PROTECTION

Fulfillment of condition	$Trusted_L=1$	$I^S_{sec1} \geq L_{DS}$	$T^S_{msg} \geq T_{DS}$	$UA_L=0$
Yes	DS/AC	DS/AC	DS/AC	DS/AC
No	DS	AC	AC	DS

TABLE II. CONDITIONS FOR DETERMINING THE POSSIBLE USE OF DS AND AC WITHIN THE FRAMEWORK OF THE IMS FOR ONBOARD MESSAGES PROTECTION

Fulfillment of condition	$I^L_{sec1} \geq L_{DS}$	$T^L_{msg} \geq T_{DS}$
Yes	DS/AC	DS/AC
No	AC	AC

The analysis of substitution of the base and/or subscriber station threat allowed to formulate the task that should be solved within the framework of the authentication procedure for the traffic participants: it is necessary to ensure the safe delivery of the integrity monitoring parameters to traffic participants while limiting the amount of information that can be transmitted within the authentication procedure.

The task of safe delivery is to solve two subtasks:

- delivery of verification parameter for the station messages $P^{S'}_{IM}$ from the station part of ALS-BR to the onboard part;
- delivery of verification parameter for the onboard messages $P^{L'}_{IM}$ to the station part of the ALS-BR or the parameter for calculating the DS/AC P^L_{IM} to the onboard part.

The solution of the first subtask can become possible in two ways. The first, the parameter $P^{S'}_{IM}$ (Figure 2a) is transmitted via the radio channel. The second, information that will allow us to calculate or determine $P^{S'}_{IM}$ at the onboard part of ALS-BR (see Figure 2b) is transmitted via the radio channel. In Figure 2a, $[P^{S'}_{IM}]_{P_A}$ means safe transfer of parameter $P^{S'}_{IM}$ to the onboard part of the ALS-BR using authentication parameter P_A.

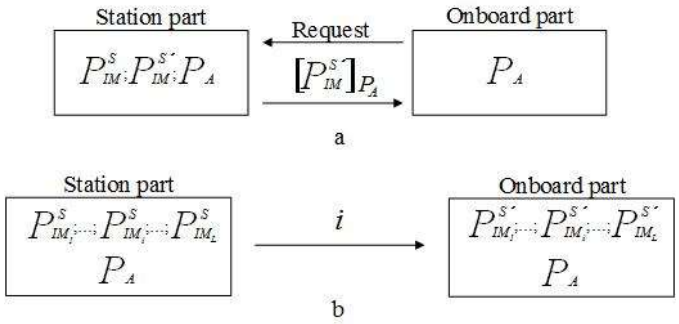

Fig. 2. Possible options for delivery of $P^{S'}_{IM}$ to the onboard part: delivery of parameter $P^{S'}_{IM}$ (a), delivery of additional information (b)

As a result of the analysis of possible solutions, the conditions influencing their choice, presented in Table 3, were determined. The parameter $p^S_{AC}/p^L_{AC} \in \{0,1\}$ determines the choice of the protection mechanism against the threat of sending fake information for station/onboard messages; I^S_{sec2}/I^L_{sec2} is the maximum amount of information that can be transmitted within the authentication from the station/onboard part of ALS-BR; $L^{S'}_P/L^L_P/L^{L'}_P$ is the size of the parameter $P^{S'}_{IM}/P^L_{IM}$ /$P^{L'}_{IM}$; $Sync\_upd \in \{0,1\}$ is the possibility of manual synchronous updating of the IMS parameters at the station and onboard parts of ALS-BR; $Ext\_ch_L \in \{0,1\}$ is the presence of a communication channel with the onboard part of the ALSR, which allows to perform the procedure of IMS parameters remote updating.

TABLE III. CONDITIONS FOR DETERMINING THE POSSIBLE SOLUTIONS OF PARAMETER $P^{S'}_{AC}$ DELIVERY TO THE ONBOARD PART OF ALS-BR

Fulfillment of condition	$p^S_{AC}=1$	$UA_L=0$	$I^S_{sec2} \geq L^{S'}_P$	$Sync\_upd=1$	$Ext\_ch_L=1$
Yes	1st/ 2nd opt.	1st/ 2nd opt.	1st/ 2nd opt.	1st/ 2nd opt.	1st/ 2nd opt.
No	1st opt.	1st opt.	2nd opt.	1st opt.	1st opt.

In order to solve the second subtask, the delivery of parameter $P^{L'}_{IM}$ or P^{L}_{IM} to the station or onboard part of ALS-BR, four possible variants were identified:

- Delivery of parameter $P^{L'}_{IM}$ (1st option) to the station part of ALS-BR;
- Delivery of information that allows to calculate or determine $P^{L'}_{IM}$ to the station part of ALS-BR (2nd option);
- Delivery of parameter P^{L}_{IM} to the onboard part of ALS-BR of the parameter (3rd option);
- Delivery of information that allows to calculate or determine P^{L}_{IM} to the onboard part of ALS-BR (4th option).

Analysis of solution options allowed to determine the conditions that affect the choice of solution, presented in Table 4.

TABLE IV. CONDITIONS FOR DETERMINING POSSIBLE TASKS OF PARAMETERS $P^{L'}_{IM}$ OR P^{L}_{IM} TO THE STATION OR ONBOARD PARTS OF ALS-BR RESPECTIVELY

Fulfillment of condition	$p^{L}_{AC}=1$	$I^{L}_{sec2} \geq L^{L}_{P}$	$I^{L}_{sec2} \geq L^{L'}_{P}$
Yes	1st/2nd/ 3rd/4th opt.	1st/2nd/ 3rd/4th opt.	1st/2nd/ 3rd/4th opt.
No	1st/3rd opt.	1st/2nd/4th opt.	2nd/3rd/4th opt.

During the analyzing of protection mechanisms against resending threats, an inequality (1) that specifies the minimum amount of information $I_{TS/SEQ}$ that must be contained in the timestamp or in the message sequence number to protect against the specified threat, and inequality (2) defining the minimum allowed frequency time tag calculations f_{TS} were obtained:

$$I_{TS/SEQ} \geq \log_2\left(\frac{K_{msg} * T_{AC}}{T_{exc}}\right), \quad (1)$$

$$f_{TS} \geq \frac{K_{msg}}{T_{exc}}, \quad (2)$$

where K_{msg} is the number of messages transmitted via the radiochannel during the exchange period T_{exc}; T_{IM} is the duration of integrity monitoring parameter used to protect K_{msg} messages. At the same time, the value of parameter K_{msg} depends on the presence of mechanisms for determining the direction of message transmission and the identification of the sender in the ALS-BR. It was concluded that if the mechanism of time stamps or message sequence numbers has already been implemented at the application level of ALS-BR, then if inequalities (1) and (2) are fulfilled for it, it can be used to protect critical information within the IMS.

In case of ready mechanism absence, the choice between time stamps and message sequence numbers will be determined in accordance with the conditions presented in Tables 5 and 6. The parameter $time\_equip \in \{0,1\}$ determines the availability of additional equipment at the station and onboard parts of ALS-BR to determine the exact time; I_{sync} is the amount of information that must be transmitted via radio channel within the authentication procedure to synchronize the values of the sequence numbers between the station and onboard parts of the ALS-BR; I_{TSmin}/I_{SEQmin} is the minimum amount of information that should be contained in the timestamp/message sequence number within the IMS; $I^{S}_{sec3}/I^{L}_{sec3}$ is the maximum amount of information that can be contained in the timestamp/sequence number to protect station/onboard messages; T_{conn} is the admissible time for connection establishment and the transmission to the critical information transfer.

TABLE V. CONDITIONS FOR DETERMINING THE POSSIBILITY TO USE TIME STAMPS AND SEQUENCE NUMBERS WITHIN IMS TO PROTECT STATION MESSAGES

Fulfillment of condition	$time\_equip=1$	$I_{sync} \geq K_{msg}(I_{TSmin}-I_{SEQmin})T_{conn}/T_{exh}$	$I^{S}_{sec3} \geq I_{TSmin}$
Yes	*TS/SEQ*	*TS*	*TS/ SEQ*
No	*SEQ*	*SEQ*	*SEQ*

TABLE VI. CONDITIONS FOR DETERMINING THE POSSIBILITY TO USE TIME STAMPS AND SEQUENCE NUMBERS WITHIN IMS TO PROTECT ONBOARD MESSAGES

Fulfillment of condition	$time\_equip=1$	$I_{sync} \geq K_{msg}(I_{TSmin}-I_{SEQmin})T_{conn}/T_{exc}$	$I^{L}_{sec3} \geq I_{TSmin}$
Yes	*TS/SEQ*	*TS*	*TS/ SEQ*
No	*SEQ*	*SEQ*	*SEQ*

Analysis of updating the security parameters of the IMS task has made it possible to determine the ALS-BR parameters that affect the development of update procedure. They included the possibility of manual synchronous updating of the IMS parameters at station and onboard parts of the ALS-BR ($Sync\_upd_L \in \{0,1\}$) and the presence of a communication channel with onboard part of the ALS-BR that allows to make a procedure of IMS parameters ($Ext\_ch_L \in \{0,1\}$) remote updating.

IV. CONCLUSION

The research showed that the integrity monitoring system should contain protection mechanisms against security threats of critical information to ensure traffic safety during the use of ALS based on broadcast radio channel. Digital signature or authentication codes can be used to protect against the threat of sending fake information. In order to protect against the threat of base and/or subscriber station substitution in the IMS the authentication procedure for traffic participants which ensures the safe delivery of the integrity monitoring parameters to the onboard and/or station parts of the ALSR should be used. To protect against the threat of resending information timestamps or sequence numbers of messages should be used. In addition, as the use of DS or AC is supposed to protect critical information, the procedure for updating integrity monitoring parameters should be provided in the IMS.

Obtained conditions that affect the choice of protection mechanisms and update procedures depend on the properties and parameters of the ALS-BR system, determined by the operating

conditions of the system, the radio communication system used, the software and hardware and the current normative base [17, 18]. A large number of conditions that affect the process of constructing the IMS makes it possible to conclude that the construction of a unified IMS, the use of which would be possible to protect any ALS-BR, is a difficult task. In general, to ensure traffic safety when ALS-BR is being used, a IMS which considers its parameters and features should be built. Thereby the purpose of further research on this topic should be the development of methodology for constructing the IMS that are applicable in ALS-BR, which would consider the properties and features of ALS systems of this class.

REFERENCES

[1] Flammini F. Railway Safety, Reliability and Security: Technologies and Systems Engineering. IGI Global, 2012, 487 p.

[2] Liudvinavičius l., Sładkowski A. New possibilities of railway traffic control systems. Transport Problems, 2016, Vol. 11 , Iss. 2, pp. 133-142. DOI: 10.20858/tp.2016.11.2.13.

[3] Flammini F. Automatic Train Protection Systems. Ind Eng Manage, 2013, Vol.2, Iss. 5. DOI: 10.4172/2169-0316.1000120.

[4] Theeg G. Railway Signalling & Interlocking: International Compendium. Eurailpress, 2009. 448 p.

[5] Tilk I.G. ALS s ispol'zovaniem radiokanala *[ALS using radio channel]*. Avtomatika Svyaz' Informatika *[Automatics Communication Informatics]*, 2010, N 7, pp. 7-9. (In Rus).

[6] Bakurkin R., Bezrodnyi B., Korotin A. Protivodeystviye komp'yuternym atakam v sfere zheleznodorozhnogo transporta *[Counteraction to computer attacks in the field of railway transport]*. Voprosy kiberbezopasnosti *[Cybersecurity issues]*, 2016, N 4(17). pp. 29-35. DOI: 10.21681/2311-3456-2016-4-29-35.

[7] Konyavskiy V., Epishkina A., Korotin A. The design of integrity monitoring and reliability verification system for critical information, transmitted in automatic train signaling system, based on DMR-RUS radio channel. Procedia Computer Science, 2016, Volume 88C, pp. 318-323. DOI: 10.1016/j.procs.2016.07.442.

[8] Kostogryzov A., Atakishchev O., Stepanov P., Nistratov A., Grigoriev L. Probabilistic modelling processes of mutual monitoring operators actions for transport systems. In: 2017 4th International Conference on Transportation Information and Safety (ICTIS). 8-10 Aug. 2017. IEEE, 2017. pp 865 - 871 DOI: 10.1109/ICTIS.2017.8047869.

[9] Vorobiev E.G., Petrenko S.A., Kovaleva I.V., Abrosimov I.K. Organization of the entrusted calculations in crucial objects of informatization under uncertainty. In Proceedings of the 20th IEEE International Conference on Soft Computing and Measurements (24-26 May 2017, St. Petersburg, Russia). SCM 2017, 2017, pp. 299 - 300. DOI: 10.1109/SCM.2017.7970566.

[10] Konyavskiy V., Epishkina A., Korotin A. The design of integrity monitoring and reliability verification system for critical information, transmitted in automatic train signaling system, based on DMR-RUS radio channel. Procedia Computer Science, 2016, Volume 88C, pp. 318-323. DOI: 10.1016/j.procs.2016.07.442.

[11] Korotin A. Analiz ugroz bezopasnosti otvetstvennoy informatsii, peredavayemoy sistemoy ALS na baze radiokanala *[Analysis of security threats of critical information transmitted by the ALS system based on radio channel]*. Bezopasnost' informatsionnykh tekhnologiy *[Security of information technology]*, 2017, N2, pp. 42-49. DOI: 10.26583/bit.2017.2.05.

[12] Canetti R., Garay J., Itkis G., Micciancio D., Naor M., Pinkas B. Multicast security: a taxonomy and some efficient constructions. In Proc. 18th Annual Joint Conf. of the IEEE Computer and Communications Societies (INFOCOM '99), IEEE, 1999. Vol. 2, pp. 708–716. DOI: 10.1109/INFCOM.1999.751457.

[13] Salem M.B. Towards Effective Masquerade Attack Detection. Columbia University, 2012, 187 p.

[14] Aura T. Strategies against replay attacks. In Proceedings of the 10th IEEE Computer Society Foundations Workshop. IEEE, 1997, pp. 59–68. DOI: 10.1109/CSFW.1997.596787.

[15] Syverson P. A taxonomy of replay attacks. In Proceedings of the Computer Security Foundations Workshop (CSFW97). IEEE, 1994, pp. 187–191. DOI: 10.1109/CSFW.1994.315935.

[16] Shubinsky I., Zamyshlyaev A. Risk Management System on the Railway Transport. In Proc. of the 2016 Second International Symposium on Stochastic Models in Reliability Engineering, Life Science and Operations Management (15-18 Feb. 2016), IEEE, SMRLO, Beer-Sheva, Israel, 2016, pp. 481-486. DOI**:** 10.1109/SMRLO.2016.84.

[17] Schneier B. Applied Cryptography, Protocols, Algorithms, and Source Code in C. John Wiley & Sons, Inc., 1994.

[18] Barabanov A., Markov A. Modern Trends in The Regulatory Framework of the Information Security Compliance Assessment in Russia Based on Common Criteria. In Proceedings of the 8th International Conference on Security of Information and Networks (Sochi, Russian Federation, September 08-10, 2015). SIN '15. ACM New York, NY, USA, 2015, pp. 30-33. DOI: 10.1145/2799979.2799980.

[19] Markov, A., Luchin, D., Rautkin, Y., Tsirlov, V. (2015). Evolution of a Radio Telecommunication Hardware-Software Certification Paradigm in Accordance with Information Security Requirements. In Proceedings of the 11th International Siberian Conference on Control and Communications (Omsk, Russia, May 21-23, 2015). SIBCON-2015. IEEE, 1-4. DOI: 10.1109/SIBCON.2015.7147139.