Digital technologies and artificial intelligence to approach creation of transport security organization systems

Tatiana Ksenofontova¹, Tatiana Kosheleva¹, and Yuan Meng²

¹Emperor Alexander I St. Petersburg State Transport University, Moskovsky pr., 9, 190031 Saint Petersburg, Russia
²Lanzhou University, 222 South Tianshui Road, Lanzhou 730000, Gansu Province, P.R.China

Abstract. The article analyses new elements used and planned to be used in security systems at railway transport facilities and proves the possibility and necessity of adapting them to all modes of transportation. Basing on the analysis, the authors propose prerequisites for creation of an integrated information transport system providing end-to-end access to information about passengers, seers-off and welcomers at all the modes of transport and throughout the country. It is also suggested that the end-to-end integrated information transport system include such elements as the unique genomic information of every passenger, welcomer or seer-off. The authors also consider feasibility of implementing a risk-oriented management system to provide automated solution of tasks of identifying, analyzing and forecasting probability of negative consequences of risky managerial solutions in the case of non-compliance or violation of safety precautions.

1 Introduction

The article will present the authors' justifications for the need to implement an organization system of security systems at objects of transport infrastructure and all the modes of transportation is due to deterioration of information security and risk of possible anti-social behaviour of passengers. Therefore, there is an objective need to create an integrated passenger security system in the conditions of unmanned traffic both on the railway and in the air, and, in the nearest future, on the water ways and motor roads, which means that the necessity is also due to availability of technological capacities for developing and launching hardware and software complexes to provide passenger security in the context of fully unmanned traffic at MCC.

2 Methods

* Corresponding author: tyuKsenofontova@mail.ru
For purposes of researching the process of creation of the transport security system, the authors used methods of analytical and scientific abstraction, a complex approach and a logical method toolkit.

Researching the process of creation of the transport security system starts with the analysis of the available security systems aimed at monitoring "anti-social passenger behaviour", involving complex and analytical approaches [1].

Every working day, 242 pairs of trains run on the Moscow Central Circle (MCC) launched in 2016 (the number being 211 on the weekends), though the length of the MCC is only 54 km. Today, there are 31 stations opened within the MCC, 148 mln passengers being carried in 2019. For the five years of MCC operation, there have been some incidents. In June 2020, there was a conflict between passengers of a brand train "Lastochka" because of loud playing of a cartoon on a tablet, in February 2021, a criminal case was initiated by law enforcement bodies on deliberate infliction of grievous bodily injury after a fight transport security inspector and three free riders at the MCC station "Rostokino". Nowadays, all the "Lastochka" brand trains (joint venture of the German Concern «Siemens» and «Sinars» group) at the MCC are equipped with video surveillance systems which transmit information to the driver's control panel, who monitors the situation on the train and in the case of an "anti-social behavior" can take measures [2]. However, this does not remove the problem.

It is necessary to create an integrated security system, which is especially relevant in the context of difficult epidemiological situation, and for purposes of arranging information digital security within the transport infrastructure and in the context of QR code - to safeguard passenger data bases. One of the elements of the integrated security system can be a hardware and software complex (so called "artificial intelligence"), which is under development and is to be launched within the "unmanned traffic" project at the MCC, where it is going to provide distant analysis of passengers' behaviour. The artificial intelligence will be able to identify "anti-social" behaviour and report thereon to the Russian railroad (RZD) central controller. The new hardware and software complex is being developed within the project on creation of the unmanned brand train "Lastochka" by the Research and Design Institute of Informatization, Automation and Communication in Railway Transport (NIIAS, where the RZD is a 75%stake holder) [3]. Trials of the new hardware and software complex as one of the elements of the integrated security system within the brand unmanned "Lastochka" train are planned for 2022. Brand "Lastochka" trains that are currently in operation can also be equipped with this complex, however, the current project of arranging the integrated transport security system will involve only unmanned electric trains.

The new hardware and software complex ("artificial intelligence") is to identify "anti-social" behavior of passengers automatically and in real time on the basis of intellectual processing and analysis of video images from the video surveillance cameras and acoustic (verbal) information (screams, signs of aggression, tone of voice and manner of speech), explosions and other loud sounds irrelevant for the environment inside the train. The new hardware and software complex must be able to independently recognize passengers' deviant behavior both inside the trains and on the platforms basing on the video flow from the cameras. In June 2021 two brand "Lastochkas" trains were equipped in accordance with the third automation level (GoA3) as part of a pilot project (and underwent about 2 thousand tests under different weather conditions), [4]which implies automatic train movement and halt, though human involvement is required to open and close the doors and provide security in emergency situations.

3 Results

RZD is planning to launch unmanned "Lastochkas" on the MCC in 2024. Buy this time, all the "Lastochka" trains should be unmanned. According to the general director of the state
monopoly O. Belozerov, certification of these trains is scheduled for 2022. Certainly, the project does not finish at this point and upon achieving the fourth automation level (GoA4) at the MCC, the control system is to run the whole complex of the train driving, monitoring and the diagnostics of the board equipment, open and close the doors automatically, with a possibility of three mode driving: by the driver from the train-driver's cabin, distantly (from the operator's console) and automatically [5]. At the present time, the brand train "Lastochka" with maximum degree of automation (GoA4) is being developed (unmanned trains are to carry passengers along the MCC with a 3-minute interval against 4 minutes now), the works should be finished in the middle of 2022, after which it should be tested for 1 year, so certification of this train is planned to be completed by 2023.

Only afterwards the decision can be made on replicating such "Lastochkas". After implementing a new hardware and software complex equipped with updated additional video surveillance cameras and doorway cameras installed to control passengers' behavior during their getting on and off the carriage and provide complete functioning of the security system, the information is transmitted to the unified RZD control center [6].

This project aimed at developing one of the elements of the transport security system and induced by the threat of passengers' "anti-social behavior" should then be adapted and installed at other transportation modes - air, water and cars, as well as at the transport infrastructure not yet covered by this idea. Unmanned projects are being developed and tested both within the motor and air transport, except for the hard- and software complex (so called "artificial intelligence") with the fourth degree of automation (GoA4), which implies that the transport complex / transport infrastructure control system provides overall control from driving the vehicle, monitoring, diagnostics of the on-board equipment to automatic locking (unlocking), opening and closing the doors at all means of transport [7]. However, it has so far been relevant only for the railway transport, though feasibility of its use to increase security both on a particular transportation mode and within the whole transport infrastructure is quite evident.

As for arranging the integrated information security system, it is worthwhile considering a possibility of using genomic information about the passengers who have proven themselves as offenders of the public order, for early detection of possible "anti-social behavior" and prevention of transport offenses, especially on the air transport. The authors think that complex usage of this information base is absolutely essential for improving security and security system both on a particular transport mode and within the transport infrastructure on the whole.

For the last five years there has been an increase in security costs (including information security) of Russian transport companies. Implementation of cyber threats bring them to understanding that control over information security provides continuity of business processes, safety of funds and data, strengthens the reputation and therefore decreases costs of elimination of these and other consequences of cyber threat implementation. Information security is both a result and a process [8].

Another element of the integrated information security system for transport and objects of transport infrastructure is application of the system of monitoring and control of information security events (Security Information and Event Management - «RusiEM»). It is considered that implementation of the «SIEM-system» to identify and prevent threats through analyzing events by the network devices, security solutions, workstations, servers and apps is feasible after all the necessary protective instruments have been installed and IT infrastructure arranged.

However, in this case, it can be argued that a transport organization might have already lost consolidated control and monitoring of information security events and implementation of the "SIEM-system" turns into a large project, which might last a year or more. "SIEM-system" can be used both at the earliest stage of building the IT and IS infrastructure and in
a transport company with the existing IT and IS infrastructure, though in this case its implementation may involve more resources, because at the primary stage of IT and IS infrastructure development monitoring and control of incidents will be organically arranged from the very beginning. "SIEM-system", which makes it possible to identify and to a particular extent prevent external and internal security threats, thanks to its ability to analyze events from the network devices, is nowadays in high demand both in the vehicle and within the transport infrastructure, being relevant for all modes of transportation, especially in the context of expanding digital data on passengers and necessity of confidential storage and usage thereof, the more so if there is a fundamental decision on collecting unique genomic information on any passenger and seers-off [9].

We can consider one more element of the integrated information security system in transport and objects of the transport infrastructure, namely implementation of new technologies of protecting corporate workplaces.

Compatibility of products, which guarantees the users accessibility to product functions in joint solutions of "Aktiv" and "Getmobit" companies, is one of the stages of deep technology integration of the above-mentioned companies in work environment projects based on the innovative "smart workplace" concept implying specific requirements to information security. A universal hybrid docking station «GM-Box», which combines functions of a "fine" client and an IP video telephone is intended for creating in organizations a unified digital workspace.

Certified means of cryptographic protection «Rutoken» integrated with the «GM-Box» docking station and «GM Smart System» platform solve problems of identification and authentication of users and creation of the electronic signature for electronic documents without installing additional software for «GM-Box» and complex settings in transport and other companies [10]. It seems feasible to propose the following collaboration scenarios for transport companies: identification and authentication of users at the «GM-Box» universal docking station using «Rutoken» tokens and smart cards, since usage of their hardware and software components in the process of identification and authentication considerably increases security of the information system against unauthorized access, as in order to get access to the system, one should not only know the user's password, but possess a physical device (a token or a smart-card), and one can easily identify theft thereof if this happens.

Expanded usage of a universal hybrid docking station «GM-Box», combining functions of a "fine" client and an IP video telephone and intended for creating in organizations a unified digital workspace allowing for identifying passengers, seers-off and welcomers, is highly demanded at all modes of transportation from the point of view of improvement of the security system in transport and within the transport infrastructure. It makes it possible to provide functioning of the "SIEM-system" and increases protection of the information system of the transport company against unauthorized access, and in the future, the integrated information transport system with end-to-end access to the information about passengers, seers-off and welcomers at all modes of transportation all over the country.

As part of the formation of an integrated transport information system of end-to-end access to information about passengers, escorting and meeting passengers on all modes of transport throughout the country, it is also advisable to consider the introduction of the so-called load testing of client web applications and IT infrastructure, on the stable operation of various systems and applications which many factors in the activities of transport organizations depend: sales, brand reputation, customer loyalty, etc [11].

To maintain the smooth operation of an integrated information transport system and to ensure uninterrupted end-to-end access to information, it is necessary to regularly check the readiness of online resources to work with a large number of users and resistance to external threats. Protection of web-applications and IT-infrastructure from external threats is provided by a number of innovation-oriented companies, which allow providing protection from all
types of "DDoS-attacks" and also help to get rid of parsing, password matching, creation of fake requests and orders, automated redemption and reservation of goods.

One of these innovative companies is "ServicePipe", which specializes in detecting anomalies in network traffic, as well as in protecting against "DDoS attacks", hacking and data theft of customers and transport companies. As well as a specialized service provider "Infosecurity", which has been providing information security, IT and consulting services for over 10 years. In October 2021, a new agreement on technological partnership came into force, which will provide a comprehensive security of online resources from DDoS-attacks of various types, as well as identifying bottlenecks in the logic and application infrastructure in the emerging integrated transport information system of end-to-end access to information about passengers, escorting and greeting on all types of transport.

Services to protect against all types of "DDoS-attacks" will be available to transport companies-partners, passengers in the format of stress test, which allows you to assess the performance of the current perimeter of protection for resistance to "DDoS-attacks. Performance testing service is relevant for assessing the performance of systems and applications with increased user load.

Through the use of Web application and IT infrastructure testing, individual test scenarios can be implemented as part of a comprehensive end-to-end information transport system and generate a wide range of security system workloads. Then, as a result, get the results of the identification of bottlenecks and develop measures to address identified weaknesses in the security of information used in advance.

The business needs of the process of forming an integrated transport information system of end-to-end access to passenger information on all modes of transport in the near future will greatly exceed the capabilities of the IT departments of transport companies. The shortage of IT professionals and the gap between business users and information technology is constantly increasing. And it will increase with the speed of geometric progression. At the same time, sluggish corporate systems, primarily transport systems, will no longer be able to provide rapid transformation of business processes in the formation of a new integrated transport information system of end-to-end access to information [12].

The formation of an integrated information transport system of end-to-end access to an interactive digital management platform will be significantly hampered without the use of synergistic opportunities of creative entrepreneurship. Creative entrepreneurship in information technology is aimed at improving information security and unlocking the possibilities of artificial intelligence. In September 2021 the Russian Government approved the Concept of development of creative (creative) industries and mechanisms of implementation of their state support.

Among the tasks of the Concept, besides the creation of system conditions for the development of Russian creative entrepreneurship, the formation of "creative laboratories" is traced. The functioning of creative laboratories as a new infrastructural element is aimed at the accumulation and qualitative active growth of the information component in the format of "new knowledge" thanks to the possibilities of artificial intelligence embedded in "cultural clusters" [13]. Cultural clusters are experimental development platforms providing on preferential terms equipped laboratories, studios for creative projects of information security, which are expected to bring to a qualitatively new level - the noosphere spatial level - the format of safe data accumulation and operation.

Apart from the above-mentioned elements of the integrated information security system in transport, involving all the objects of transport infrastructure, the integrated information transport system with end-to-end access to information can additionally include a risk-oriented management system providing automated solution of problems of identification, analysis and forecast of the probability of negative consequences of risk management
solutions in the case of non-compliance or violation of the safety rules, as part of risk-management, which employs data warehouses used nowadays by credit institutions.

4 Discussion

The authors believe that specifics of implementation of the risk-oriented management system as part of the integrated information security system in transport consist in the fact that evaluation of the efficiency of managerial decisions directed at choosing an alternative managerial decision in the situation of high risk probability in a negative and unsafe transport situation, which are due to negative circumstances resulting from incompliance or violation of the safety rules, must imply forecasting of all the significant risks, each risk correlating with the forecasted expected and unexpected losses [14].

The authors consider, that main approaches to creation of the security management systems at transport infrastructure facilities, as well as at all modes of transportation, imply creation, usage and adaptation of a number of elements discussed in the article, which can help improve the situation with information security both in the transport companies and with the passenger data. They can also help monitor and stop dangers connected with passengers' "anti-social behavior" in due time. Besides, it is advisable to consider adaptation of a digital platform for choosing risk-oriented management for purposes of automation of a complex for solving problems of identification, analysis and forecast of the probability of negative circumstances of risk-management decisions in the course of incompliance or violation of safety rules as part of designing the integrated information transport system with end-to-end access to information about passengers, seers-off and welcomers at all the modes of transportation throughout the country.

Thereby the authors' suggestion within the framework of developing approaches to creation of the security management systems at transport infrastructure facilities is to consider a possibility of application and adaptation of a hardware and software complex (so-called "artificial intelligence") with the fourth level of automation (GoA4) at all the modes of transportation, which will help to monitor and stop dangers connected with "anti-social" behavior in due time and at all modes of transportation. Also, as part of creation of the information digital protection system for both internal information and constantly stored and replenished customer databases, it is advisable to consider a possibility of implementing technologies for protecting corporate workplaces by creating working environments based on the innovative conception of "smart work place" with special information security requirements.

The authors also propose to consider feasibility of implementing the risk-oriented management system as part of the integrated information security management system in transport in the format of adaptation of the digital platform of choice and risk-oriented management to provide automation of a complex for solving problems of identification, analysis and forecast of the likelihood of negative consequences of risky management decisions that may arise in incompliance or violation of the safety rules [15]. All the elements proposed as part of developing approaches to creation of the security management system at transport infrastructure facilities will contribute to creation of the integrated information transport system with end-to-end access to information about passengers, seers-off and welcomers at all modes of transportation all over the country using the unique genomic information for every passenger, seer-off or welcomer.

In the process of forming an integrated information transport system of end-to-end access to information on an interactive digital management platform, a systematic approach to the development of information cluster infrastructure will be necessary. At the same time, it is impossible to achieve a systematic approach without building a multi-level effective system of intellectual property protection.
References


