**REPORTS OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN**
ISSN 2224-5227
Volume 2, Number 318 (2018), 23 – 30

UDC 004.056 (045)

Berik Akhmetov

Caspian State University of Technologies and Engineering named after Sh. Esenov, Aktau, Kazakhstan
berik.Akhmetov@yu.edu.kz

STATUS, PERSPECTIVES AND MAIN DIRECTIONS OF THE DEVELOPMENT OF CYBERSECURITY OF INFORMATION AND COMMUNICATION TRANSPORT SYSTEMS OF KAZAKHSTAN

Abstract. The article contains the results of a comparative analysis of previous studies in the field of cybersecurity of information and communication transport systems. The analysis was carried out in the context of the solved problem of the further development of methods and models for the recognition of cyber threats, anomalies and attacks directed against information and communication transport systems, as well as assessing the risks of information security of the transport industry as one of the components of the critical infrastructure of the Republic of Kazakhstan. The urgency of the task is also caused by the formation of a unified information and communication environment of the transport industry in Kazakhstan, the introduction of new and modernization of existing information systems in transport in the conditions of increasing the number of destabilizing effects on the availability, confidentiality and integrity of information.

Key words: information and communication systems, information security, critical computer systems, information security system, cyberattack detection systems.

Introduction

In the condition of globalization, there is arisen significantly the role of the transport infrastructure for ensuring the development of trade and economic relations between countries, their cultural, tourist and sport relations, as well as international transit traffic. The participation of the Republic of Kazakhstan (RK) in international integration processes in the field of transportation is a non-alternative trend, but it must be accompanied by the creation of a modern infrastructure compatible with the infrastructure of the countries with which the RK interacts with the simultaneous protection of national interests.

The solution of these tasks is impossible without effective information support systems that integrate control processes, data processing, monitoring, communications, etc. Modern information technologies (IT) on transport in conjunction with navigation and surveillance systems provide an opportunity to track and analyze traffic flows on the railways, roads, oil and gas pipelines, air and waterways, etc. It is also possible to carry out the accumulation and analysis of the received information in intelligent transport networks, to use the data for the decision-making and operation of transport and logistics centers.

The aim of the work is a comparative analysis of previous researches in the field of cybersecurity of information and communication transport systems, in the context of the problem of the further development of methods and models for cyberthreats recognition, anomalies and attacks directed against information and communication transport systems (ICTS), and also assessment of the risks for information security branch as one of the component of the critically important infrastructure of Kazakhstan.

A review of previous researches

For Kazakhstan, the problem of information protection and information and cyber security (IS and CS) ensuring of the transport sector have a particular importance. This is primarily connected to the size of the territory and the geopolitical location of Kazakhstan, with political and socio-economic policies aimed at further strengthening of sovereignty.

Intervention in national, regional and municipal automated information and control systems on transport is a frequently mentioned threat for cyberattacks of intruders [1-4]. The high degree of human involvement in transport logistics and transportation processes control does not reduce the risks associated with cyberattacks and with unauthorized intervention in work of ICTS [4-8]. At the same time, the statistics of IS and CS incidents in the world ICTS are replenished every year, Table 1 (data are based on the analysis [9-17]).

Table 1 - Intervention in work of ICTS

№	Year	Country	Event	Describedconsequences
1	2002	United Kingdom (UK)	Unauthorized access to the service telephone connection of the railway and to the semaphore control system.	Disconnected from communication control room, a failure in the semaphore switching system [11].
2	2003	Sweden, Gothenburg	Hacking of ACS of city buses and taxi traffic.	Loss of control over the movement schedule for several hours [4, 13].
3	2014	Russia	The virus disconnected the video cameras fixing the "Strelka-ST" high-speed mode in Moscow and in the region.	The cameras are disabled for several days [11].
4	2003	USA	SQL Slammer virus violates ACS of Continental Airlines company	Cancellationofflights [2].
5	2008	China	In the Chinese city of Weifang there was arrested a man who committed the largest attack in the history of China on Chinese transport companies	Downtime of transport companies in Weifang
6	2008	Pakistan, India	Hackers from Pakistan hacked the access to the site of the Indian Railway Company	The site did not work more than 12 hours
7	2012	Russia, Netherlands, UK, USA	The hacker group Anonymous has committed cyberattacks on the servers of Gazprom, Rosneft, Shell, BP Global and ExxonMobil	In the free access there were thousands of mail accounts of employees and company data [13, 18].
8	2013-2014	Somalia, USA, UK, Norway and others.	There was released the report of a Rapid7 company on the facts of interference in the operation of GPS systems of oil platforms, tankers and container ships in the Persian Gulf and in the Aden Strait.	The facts of software failure on drilling platforms for 19 days are fixed [11, 18].
9	2016	Ukraine	Hacking the video-broadcast system in the metro in Kiev	Replacementofvideocontent

The increase of the number of cyber attacks on ICTS in recent years increased an interest to the development of effective information security systems (ISS) focused on the specifics of the transport [1, 3, 6, 8, 11, 14].

In general, the authors were focused on the problems of IS and CS of certain types of transport: aviation [1, 2]; pipeline, as an element of critical infrastructure [3-5]; automobile [6]; sea and river [7, 8]; railway [9-12]. The results of a comprehensive assessment of the role of information and cybersecurity of the transport as a component of the national security of the state and its critical infrastructures are presented in works [13-17]. However, we note that the works do not contain descriptive models that allow to identify the patterns of situation evolution related to the IS and CS on transport. Most of the researches did not have apractical implementation in the form of applied software, which would allow, in particular, to develop a specific methodological basis for organizing the ICTS protection system taking into account their specificity.

Insufficient attention to the problem of ICTS cyber security can lead to interception of control and to the failures in the dispatching control systems of the transport. As the worst result, there can be the consequences with human casualties. As an additional risk, there can be considered the lack of ICTS standardization and their components responsible for IS and CS [2, 6, 11, 13, 18].

In works [14, 16] there was analyzed the methodology of intellectual modeling, designed for analysis and decision-making in insufficiently structured situations of IS and CS of ICTS. At the current stage, the researches [13] are not brought to hardware or software implementation.

Difficult to analyze and decision-making support, regarding the ICTS protection, are the weakly formalized and structured tasks of IS and CS with the appearance of new classes of attacks [2, 4, 5, 13, 16]. In this case, the ICTS condition parameters can be represented by qualitative indicators, which is not always advisable.

Therefore, taking into account the controversy in the reviewed works, it is relevant to solve the task of carrying out new researches aimed at developing the methods and models for IS and CS of ICTS control, taking into account the peculiarities of their infrastructure, as well as dynamically changing requirements for the control of cybersecurity on transport.

Information and communication transport systems as an object of cyberattacks

The active application expansion of the IT sphere and critically important information transport systems (CIITS) in Kazakhstan, especially in the segment of mobile, distributed and wireless technologies, is accompanied by the appearance of new cyber threats. This is confirmed by the increase of the number of incidents related to cybersecurity (CS) and by the protection of information in CIITS [18, 19]. Threats are very real, because the attackers can get the opportunity to intercept passwords, separate files, geolocation information, broadcast audio and video data, monitor Wi-Fi networks, web cameras, information boards on roads and railways, stations, airports, etc.

Nowadays, many projects in the field of transport control are developing in the direction of creating of large situational centers (SC) that provide solutions for specific tasks, in particular, for the protection of CIITS. Investing of innovative projects, for example in the field of CS and information security, is characterized by a high degree of uncertainty and risk. Many enterprises and companies, engaged in CIITS service, spending a large amount of money on information security systems (ISS) and CS, do not feel confidence that the chosen investment strategy makes the ICTS infrastructure really safe.

A serious problem in the CS of CIITS area is the protection against unauthorized access (UAA). The seriousness of the problem is evidenced by the fact that even one person who has access to CIITS for a short time can completely paralyze the work of any strategic railway, seaport, gas or oil transport enterprise site, etc.

Virtually any ICTS can act as an object of attack.

In order to implement it an attacker (intruder) needs to activate the ICTS vulnerabilities. As the statistics [11, 13, 18] show, such vulnerabilities do not become less.

Nowadays, the transport industry in the whole world and in the RK, in particular, is passing through the stage of transformation and adaptation to new digital technologies. The current state of many means of informatization and automation of transport systems is still based on traditional SCADA. However, there is already an active connection to the Internet both of the vehicles themselves and of the components of the transport infrastructure: video surveillance cameras, information boards, smart stops, cloud infrastructure, etc. All these elements are vulnerable to cyberattacks. According to the data of [18], only during the period from March 2015 to May 2016 ICTS has been compromised to DoS attacks and other destructive influences by computer intruders more than 44 times.

The comprehensive nature of the tasks of the ICTS formation in RK requires their systematization and selection of priorities [19]. Today, in the transport sector of the Republic of Kazakhstan there are developed a number of industry information systems and communication networks which operate autonomously and are not interconnected (Table 2).

Almost all elements of the ICTS can become objects of cyberattacks. As the analysis of real attacks showed the following categories of objects in infrastructural solutions of information and communication systems of the transport industry are the most vulnerable [1, 4, 6, 7, 11, 14, 18]: 1) data processing centers, automated control systems for various modes of transport (SCADA, etc.); 2) peripheral equipment components (for example, information boards); 3) devices on programmable logic controllers (PLC); 4) systems and communication channels for data exchange between dispatchers and vehicles; 5) navigation systems using GPS and GLONASS.

Table 2 - Automated information and control transport systems (Republic of Kazakhstan)

Type of the transport	Name	Typical tasks	Peculiarities
1	2	3	4
Railwaytransport	ACS on RS	Automated control systems on rolling stock.	The system works on the server complex IBM Z9. There are used PLC Siemens, ABB, GE, Schneider Electric, Emerson and others.
	ACS Client	Accounting of cargo, execution of invoices, etc.	The ACS is based on the software and hardware complex P780 IBM, DBCS Oracle.
	ACS «Express-3»	In the on-line mode: requests for the information; Purchase of electronic tickets on trains of international and republican communications; and etc.	The system is based on the software and hardware complex P780 IBM, DBCS Oracle.
	ACS for RWI	Automated control system for cargo and railway wagons integrity in motion provides: video surveillance in real time with the passage of the train, the state of wagons, the presence of locking and sealing devices on the locking mechanisms of doors and hatches and so on.	Software TNS-INTEC (RK)
	Etc.		
Automobile and traffic control systems on highways	ACS logistics, software «Autograph»; Wialon Hosting software and etc.	Integration with business information systems of cargo carriers; Identification of the possibilities of cargo carriers; Access to the order pool corresponding to the parameters of the particular carrier; Formation of transportation documents; Payment for services rendered; Control of the passage of the cargo.	They work on Windows, Android platforms. there are used PLC GE, Schneider Electric, Emerson, etc.
Seatransport	Navi-Harbour 1000	The unified information system of the port community (ISPC) provides: accounting of the port's work (accounting of railway wagons, trucks and other rolling stock located in the port) preparation of electronic and shipping documents; preparation of paper transportation documents; interaction of AIS enterprises with ISPC; interaction of ISPC with customs AIS for the transfer of electronic data on the cargo; formation of statistics, reports and accumulation of the archive; others	The system is based on the hardware and software complex P780 IBM, Oracle DBCS, MySQL Work on Windows platforms. There are used PLC Siemens, ABB, GE, Schneider Electric, Emerson, etc.
Aviationtransport	ACS of SAP ERP, B2B services, E-ticket, (on the example of Air Astana and etc.)	The corporate control system based on SAP ERP of the Republican state enterprise on the right of economic management "Kazaeronavigation" provides: complex automation of business processes of financial and economic activity of enterprises; optimizes and unifies the processes of information exchange. B2B services provide: booking of passenger and cargo transportation; viewing of the flights schedule, free passenger and cargo places; executionofinvoices; others	Software SAP AG (Germany)