Journal of Theoretical and Applied Information Technology
31st July 2016. Vol.89. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

IMPROVING OF INFORMATION TRANSPORT SECURITY UNDER THE CONDITIONS OF DESTRUCTIVE INFLUENCE ON THE INFORMATION-COMMUNICATION SYSTEM

[1]LAKHNO V.A., [2]PETROV O.S., [3]HRABARIEV A.V., [4]IVANCHENKO Y.V., [5]BEKETOVA G.S.

[1,3] Department of Managing Information Security, European University, Ukraine
[2] Faculty of Management, AGH University of Science and Technology, Poland
[4] Academic Department of IT-Security, National Aviation University, Ukraine
[5] Kazakh National Technical University after K.I. Satpayev, Department of Computer and Software Engineering, Republic of Kazakhstan
E-mail: [1]lva964@gmail.com, [2]asp1951@gmail.com, [3]andr.grab@gmail.com,
[4]icaocentre@nau.edu.ua, [5]beketova_gs@mail.ru

ABSTRACT

Information-communication environment of transport (ICET) is focused on interaction with other sectors to reduce delays in transporting of goods, processing sea and river ships, containers, rail cars and cargo at border crossings through the use of electronic invoices, "Client-Bank" system, e-business, interaction with the clients and partners and so on. Severity of system failure of this level of complexity requires new research on information security (IS) ICET with an emphasis on affordability and sustainability of systems and the integrity of the information stored and processed in information systems (IS) and automated control systems (ACS) of an industry.

The article contains the results of studies aimed at further development of methods and models recognizing threats ICET and improvement IS in the conditions of formation of a single information and communication environment, introduction of new and modernization of existing IS of transport, and increase the number of destabilizing effects on the availability, safety and integrity of information. The method of recognizing threats based on discrete treatments using the apparatus of logic functions and fuzzy sets, which improvements of the recognition efficiency, create effective analysis, schematic and software solutions of integrated systems of information security (ISIS) of ICET.

Key-words: *Information-communication environment of transport; Protection of Information; the data processing system; security policy; highly reliable information processing; mathematical models.*

1. INTRODUCTION

Active expansion of information-communication environment of Transport (ICET), especially in the segment of mobile, distributed and wireless technologies, accompanied by the emergence of new threats to information security (IS), as evidenced by the growing number of incidents related to information security and protection of information and discovered vulnerabilities in information systems (IS) and automated control systems (ACS). The threats are real, since criminals can get the opportunity to intercept passwords individual files, geolocational information, broadcast audio and video data, control the Wi-Fi-networks, webcams, information boards on roads and railway tracks, railway stations, airports and others.

Considering the above mentioned, is to stay on the premises of ICET protection as an integral part of national security. [1-4]

First, the importance of the transport sector (TS) in the national security and economy of individual countries. [5-7]

Secondly, the need to ensure the security of the transport process and its information component, whose role is growing.

Thirdly, with the integration of Eastern Europe to the Eurasian transit corridors, information resources become for the industry of the same importance as

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

material and production.

For the fourth, a significant vulnerability and IS ACS of transport sector (TS), due to the emergence of new methods of attacks on information, including Cyber-attacks (CA), widespread wireless communications, navigation systems using GPS, GLONASS, GALILEO, video surveillance systems (SC), communication technologies GSM-R, VSAT, supervisory control systems (SCADA, HMI), PLC in various modes and others. [7, 8, 9, 10]

For the fifth, the need to develop principles of building a secure ICET management of techniques and information and computational process, based on a comprehensive application of existing tools and methods of protecting and storing information in the interests of supporting sustainable efficiency and managing IP traffic.

2. FORMULATION OF THE RESEARCH PROBLEMS

The research purpose is the construction of new models and methods to protect information-communication environment of transport on the basis of the constant threats recognition of increasing the number of destabilizing influences.

3. REVIEW OF THE LITERATURE

The object of the attack to information may be any of the elements ICET. However, in general all the elements ICET can be assigned to one of the following categories: data processing centers (DPC), ACS, IS systems SCADA, HMI; peripherals and PLC; systems and channels for communication

The research of IS are dedicated such works: V.P. Babak, D.S. Biryukova, V.S. Blintsov, G.B. Vilskoho, A.V. Yesikova, A.A. Kornienko, O.H. Korchenko, V.A. Ryndyuk, A.I. Stasiuk, V.P. Kharchenko and others. However, in Ukraine these studies have fragmented character. [5, 6, 7, 8, 10]

In intruders have several entry points to compromise IS or ACS TS. ASC TS may be contaminated in various ways, such as virus (exploit) can be implemented via USB-connection or through a network interface.

Typically, the amount of detected vulnerabilities correlated with the number of published exploits, such as in February 2011 to September 2013 was published 150 exploits [7, 9, 10], i.e., it is eight times more than in the period from 2005 to 2010.

Vulnerability of ASC, SCADA, HMI, PLC is due to lack of security mechanisms in industrial protocols and systems of a project, vulnerability of software (SW) and its incorrect configuration. The need for integration with external networks (corporate, WAN, Internet), wireless networks and public information technology - operating systems, network protocols and services Remote access - do not contribute to the safety of ASC. [11, 12, 13, 14]

4. MATERIAL AND METHODS

4.1. Information-communication environment of transport an as object of attacks on information resources

For managing IS and ACS of transport is characterized by the following kinds (Table. 1): onboard equipment installed on moving objects ICET (means of remote monitoring, measurement, and so on.); means mounted on fixed infrastructure (means of remote monitoring, measurement, and so on.); remote-controlled executive and indicative devices (devices and units); servers for processing and storage; situational, operational and dispatch center's; means of communication – Internet, Network GSM/ GPRS, GSM-R, VSAT, satellite communications; information and telecommunication equipment, providing a secure information interaction with external information systems.

The structure of the technological complex IS and ACS TS may include various technical systems and tools: systems and tools coordinating time, meteorological, and so on., types of support; systems, equipment, lines and networks and data; systems and remote monitoring equipment; systems and means of collection, storage and processing; computerized systems and controls; system and display facilities and bring information; other technical software and hardware.

Most of the systems and tools are used to form a feedback channel with an operator, and the controlled technical components of transport system.

Virtually every information or information management system, including transport, may be the subject of unauthorized access, that is the attacker set of actions designed to violate one of the three properties of information – confidentiality, integrity or availability. [10, 15, 16, 17, 18, 19]. After identifying the industrial and transport SCADA and IS such complex viruses as Stuxnet (2010), Duqu (2011), Flame (2012), Careto (2014) there was a sharp jump of interest in information security critical ACS, AIS and IP.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: The Goals, Objects And Subjects Of Attacks On Information In ICSTF

The aims of the attack on the ICSTF can be	Cyber spying – unauthorized transmission via hidden (undeclared) channels of data, programs DEIIS, MIS, IS, ASK TS or geographic coordinates (GPS or GLONASS and other technology)
	Cyber audit – development of scenarios cyber- attacks, hacking and "friendly" cyber- attacks, search of ICET TS vulnerabilities
	Cyber fraud – "sale" of counterfeit electronic tickets, breaking of automatic machines ticket sales and receipts of baggage payment, hacking of account meters of cargo, energy and automatic flow and refuelling etc.
	Cyber sabotage – reducing the capacity of road, rail, and pipeline routes, in particular, to a complete stop of transport processes.
	Cyber sabotage – reducing the capacity of road, rail, and pipeline routes, in particular, to a complete stop of transport processes.
The aims of the attack on the ICSTF can be	Railway
	Automobile
	Sea and river
	Pipeline
	Municipal
	System of Navigation and Logistics
	The objects of cyber-attacks on transportation systems can be systems of automated traffic control and management (IS, ACS, SCADA, PLS, HDI), responsible for creating safe routes of rolling stock (RS) systems of safe movement of RS and safe passage for crossings r/t, the system of protection and regulation of power supply, automatic fire extinguishing systems and thermal stabilization, automation systems in sea and river ports, train depots, et al., communication system GSM-R, VSAT et al., as well as operators, service staff – managers, queues, and drivers r/t drivers, crew and aircraft
Attacking side	The hackers, competitors, insiders, organized criminal groups, security forces, armed forces of foreign states (cyber troops). The level of "armament" (technical equipment) and competence (information awareness) of "attacker" may be very high.

4.2. Information Security Of Transport As A Component Of National Security

Information security of TS has never been released as a separate type of national security. Moreover, the information security of transport industry (IS TI) cannot exist outside of national security. As part of a whole, it carries heredity conceptual approaches to ensure security at the micro and macro levels, continuity of relationships, common principles and methods. Moreover, IS of transport usually has its own characteristics and specific, reflecting the industry direction and defining its place, role and importance in the structure of national security.

It is equally important the classification of IS TI, which allows selection of specific policies and strategies for its support. As initial data for classification it is advisable to select types of transport subsystems as objects of information security with specific threats to the different modes of transport. As a result, the structure we will have IS TI, which is presented in Fig. 2.

The practice shows that these subsystems of IS are closely linked and are in dialectical interaction. In addition, we should clearly distinguish "a system of information security in transport" from "system of transportation security" as a real system structures, powers or funds that are directly involved in activities to ensure transport safety. This is fundamentally different concepts with different domains of knowledge and practice that require specific training of professionals responsible for transport security in general and its individual types.

Journal of Theoretical and Applied Information Technology
31st July 2016. Vol.89. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

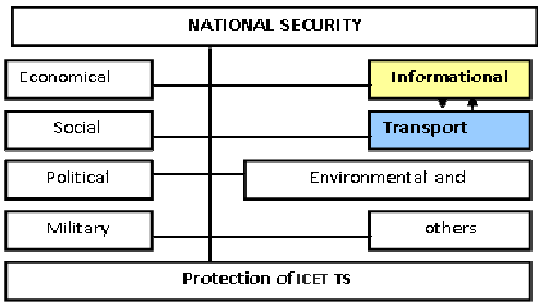

Fig. 1. Place Of IS TI In The General System Of National Security

Incomplete information about threats to information security and IS and ASC TS is twofold. Firstly, it is partial lack of prior information, even at the level of the structure of the object to attack information, which has, as a rule, stochastic nature. Secondly, the limited ability of observation of the object of recognition and attack threats, which belong to a particular class. In the extreme case it is previously known only to the total set of IS threats and ways to implement them, see. Fig. 3.

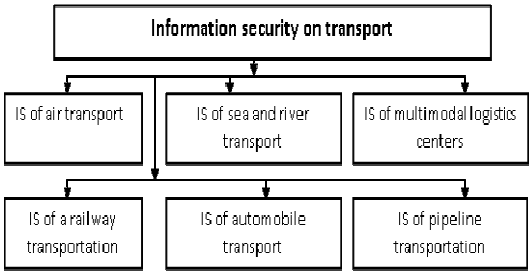

Fig. 2. The Structure Of Information Security On Transport

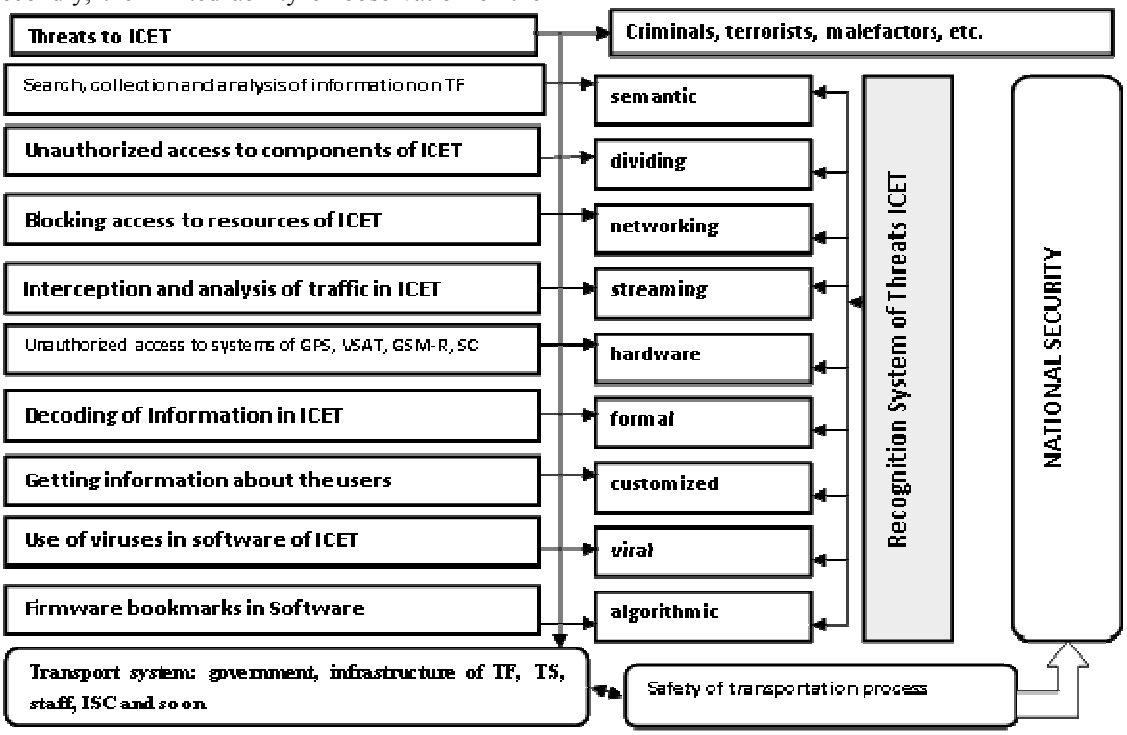

Fig. 3. Threats To ICET

However, in practice, one of the main characteristics of today's threats is that they are not activated for a long time, sometimes for two or three years. [18]. The targeted attacks, are particularly aimed at IS of enterprises, infrastructure, energy, transport, etc., is usually tailored to the environment in which they will be targeted. Modern threats are created in a way, as to circumvent the protection, and usually are not detected by signature. Development of scenarios SOI performed in compliance with all standards and technologies, the terms of reference, work design, testing, support and upgrade.

4.3. Method And Model Of Identification Threats To Information Security Of ICET

The degree of danger each threat of ICET depends on the values of a number of factors that increase or decrease the security object information security (OIS) on a particular class of threats, such

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

as cyber-attacks (CA). Factors that reduce the security of OIS, will be called risk factors, and those that enhance it – factors of security. The integrated vulnerability assessment and security of OIS is a function of its protection from every type of threats. The information which is the basis of building discrete recognition procedures threats (DRPT) IS can be presented in various forms, particularly in the form of hard understandable signs of unauthorized access $\{p_{ax1},...,p_{axn}\}$ in IS and ASC TF ranges of limit values, the input parameters of outgoing traffic, unpredictable addresses of packages, attributes, time parameters, queries, and so on [20, 23, 24].

The in the study process, taking into consideration characteristics of the subject area and formulated tasks, it was used: Boolean algebra, the theory of fuzzy sets – to develop method of intellectual detection of threats predictive and construction of discrete procedures of threats identification (DPTI) ICET. [16]

It was studied the set of objects *PA* – the number of possible targets offender in of ICET. The set *PA* is presented in a union of disjoint subsets (classes) of threats IS, realized by an offender in achieving p_a the goal.

There is a final set of objects $\{sp_{a1},...,sp_{am}\}$ with *PA* are known classes of threats which they belong (these precedents, those are objects, used for training – OVN). It should be brought under a set of values of attributes, which is a description of an object sp_{an} with RA, it is unknown to which class it belongs to, to determine the class and, therefore, work to build a GIS so that it could relist effectively to the threat within this class.

Vulnerabilities also divided into classes according to the vulnerability sources, classes into groups and subgroups for displays.

The main objective of building DPTI is to search for informative signatures (or fragments of descriptions) of objects. In DPTI IS such fragments are considered informative, which are meet in the descriptions of objects in one class, but do not meet the descriptions of objects in other classes of IS threats.

When building the DPTI IS it was introduced into use the notion of elementary classifier, which is defined as a fragment of describing OVN. For each class of IS threats is being built the set of elementary classifiers with predetermined properties.

The method of solving (decisive) rule $gov(p_{axi})$ for intellectual recognition of threats ICET in which recognition would be conducted with a minimal number of errors.

The threat of changing the state of IS ICET was presented in the following form:

$$S_R = \langle EUM^*, SDN, RDN, ADN, MIF, IR \rangle, \quad (1)$$

Where EUM^* – set of entities, comprising: a subset of nodes ICET TS - um^* (potential vulnerabilities) [13, 18, 20, 21, 22, 26];

SDN – set of objects ICET TS;

RDN – set of graph edges states of the system S_R, including those that meet the user access rights to EUM^*;

ADN – set of graph edges states of the system S_R, corresponding to the received access to EUM^*;

MIF – set of graph edges states of the system S_R, corresponding information flows between the EUM^* ($um^* \subset EUM^*$);

IR – function hierarchy of EUM^*.

The main feature of proposed method of intelligent recognition of threats of ICET TS, is the possible to obtain results in the absence of information on the distribution function of the values of the signs and the presence of small training samples.

The main objective of building DPTI is in search of informative subsigns (or fragments of signs).

Informative are considered fragments that display certain patterns in the description of objects used for training. In DPTI for Information Security (IS) are considered informative pieces that are found in the descriptions of the class objects, but not found in the descriptions of the objects of other classes of threats to information security. Considered fragments tend to have a meaningful description in terms of designing DPTI.

As the importance of informative signs attacks on ICET TS will consider value:

$$IZ_{p_{axj}} = \frac{\sum_{\substack{(sp'_a, NP_{pa}) \in MC^{AL}(KL) \\ p_{axj} \in NP_{pa}}} vop_{(sp'_a, NP_{pa})}}{\sum_{\substack{(sp'_a, NP_{pa}) \in MC^{AL}(KL) \\ p_{axj} \in NP_{pa}}} vop_{(sp'_a, NP_{pa})}}, \quad (1)$$

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Where $vop_{(sp'_a, NP_{pa})}$ - significance function of elementary Classifier (EC) threats to IS ICET;

MC - a set of all EC, generated by a set of attributes threat of attack on IS or ACS $\{p_{ax1},..., p_{axn}\}$.

NP_{p_a} - basic set of KL class features to IS attacks or ACS - $NP_{p_a} = \{p_{ax_{j1}},..., p_{ax_{jr}}\}$;

KL - threats classes of IS information security and ICET TS [10, 25, 27];

AL - set of recognition algorithms of threats.

Building a basic set of classifiers for the simulated class of threats which comes down to this: 1) given characteristic function; 2) built DNF that implements this functionality. 3) calculated allowable (maximum) $\Re$ conjunction, which defines the object belonging to a class of threats information security of ICET TS.

For each ratios tree output constructed fuzzy knowledge base that represent a set of fuzzy rules "if-then" that defines the relationship between input and output variables when evaluating information security of ICET TS. For fuzzy knowledge bases compiled logic equation. The rule is activated if the truth of his condition is greater than zero. [28, 29]

To assess the effectiveness of procedures recognition it was used the method of sliding control. The likelihood of recognition of threats of P_{p3} for information security of ICET TS is calculated by the expression:

$$P_{p3} = \Phi\left(\frac{0{,}5 \cdot \sum_{i=1}^{N_{pa}} \left[1 + \Phi(IZ_{p_{axj}} / 2) \cdot \log_2 n_i\right]}{2 \cdot N_{pa}}\right), \quad (2)$$

where Φ – probability integral;

N_{pa} – the number of signs of attacks on information;

$IZ_{p_{axj}}$ – informative value of signs of attacks;

n_i – number of gradations characteristics of attacks on information.

In Table. 2 was given an example of the training matrix for the knowledge base for DPTI ICET, such as IS or ACS. Using fuzzy variables allows describing the characteristics of the attack on the information and making fuzzy logical conclusion after constructing classification rules according to obtained decision tree.

For each of output ratios a conclusion tree, it was constructed fuzzy knowledge base that represent a set of fuzzy rules "if-then" that define the relationship between input and output variables in evaluating information security of ICET. For fuzzy knowledge bases it was compiled logic equation.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: Knowledge Base To Identify Threats To Information Security Of ICET TS

Attributes	Signs of attacks on information	Informational characteristic value	Univer-sum	Topics for lin-guistic evalua-tion ϕ_u ,..., ϕ_v
The set of classes of threats IS $KL = \{KL_1,..., KL_n\}$, The set of offender's goals the в ICET $PA = \{PA_1,..., PA_z\}$, The set of numbers of threats to IS, realized by the offender in achieving the p_a goal $B_{p_a} = \{b_{p_{a1}},..., b_{p_{au}}\}$, The set of numbers ISIS $N_j^{p_a} = \{n_1^{p_{a1}},..., n_j^{p_{au}}\}$, The set of possible offenders $U = \{u_1,..., u_g\}$, The set of recorded incidents $NIS = \{nis_1,..., nis_f\}$, The set of possible of attacks options $AT = \{AT_1,..., AT_q\}$, The set of algorithms (AL) recognition threats $MC = \{MC_1^{AL},..., MC_j^{AL}\}$, and other.	The set of attacks signs on information within the class of KL $p_{ax} = \{p_{ax1},..., p_{ax_{MI}}\}$.	Based on NIS and terms ϕ_u ,..., ϕ_v $-1 \le IZ_{p_{axj}} \le 1$	$[0, N_a]$ or [0,1],	uncritical, critical *or* found, partly revealed, no-found *or* fixed ISIS, unfixed ISIS *or* vulnerability found, partially revealed, non-identified, etc.
The states of systems (IS and ACS) $S_{IK} = \{S_{IK_1},..., S_{IK_m}\}$				
Methods of counteraction (ways to protect ICET) $D_{33i} = \{D_{33i_1},..., D_{33i_r}\}$				
Rules for the conclusion tree *IF* ($KL_1 \vee ... \vee KL_n \vee S_{IK_j} \vee ... \vee S_{IK_m}$) *THEN* D_{33i_r} and $\mu^{d_j}(S_{IK_i}) = \bigvee_{p=1}^{h_j}[\mu^{y_1}(y_1) \wedge ... \wedge \mu^{\phi_v}(\phi_v)]$, $p = \overline{1, h_j}$, $j = \overline{1, MI}$, where $\mu^{y_1}(y_1)$,..., $\mu^{\phi}(\phi_u)$, $\mu^{\phi}(\phi_v)$ – functions of affiliated variables y_1, ϕ_u ,..., ϕ_v to their fuzzy terms; y_1 – condition of IS {below the critical, critical, above the critical, high}; $\vee$ – logical OR, $\wedge$ – logical AND, as operations *max* and *min*.				

The rule is activated if the truth of its condition is greater than zero. The methods of compiling decision rule $gov(p_{axi})$ to determine the state of S_R systems in case of a threat to information security, are based on critical analysis of individual elements procedure of ICET TS, and determine the stages:

1) for each unit $um^* \subset EUM^*$ identify authorized users that have the right to access each entity (e.g., information array – $M_{k\,inf}$);

2) a set of EUM^*, SDN possibly IR do not change on all trajectories of the graph of the system conditions;

3) for obtaining by an attacker (subject-offender) SDN_x right of possession about the subject SDN_i for him, as a rule, necessary to get access not only to the essence of EUM_z^*, but also access to copy / read to a certain essence DYEIIS, which is the interface or port of an object process $pro \in SDN$, which makes the provision of access

Journal of Theoretical and Applied Information Technology
31st July 2016. Vol.89. No.2

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

rights SDN_i based on information in essence of EUM^*;

4) essence of EUM_z^* and eum_l is associated with the subject pro_r^m; essence of eum_l and pro_r^m, as a rule, placed on one network node, and essence of EUM_z^* and EUM_y^* can be placed on different nodes of ICET TS;

5) critical (solution) rule of *gov(x),* which describes ICET or ACS, can be represented as such (see. table. 3).

Tables 3: Decisive Rule $gov(p_{axi})$ To Determine The State Of ICET TS In The Event Of Threats To Information Security

Rule	Initial state, S_R	The resulting condition, S'_R
[illegible]	[illegible]	[illegible]

During the research was developed expert system (ES) "Analyzer threats," see. Fig. 4.

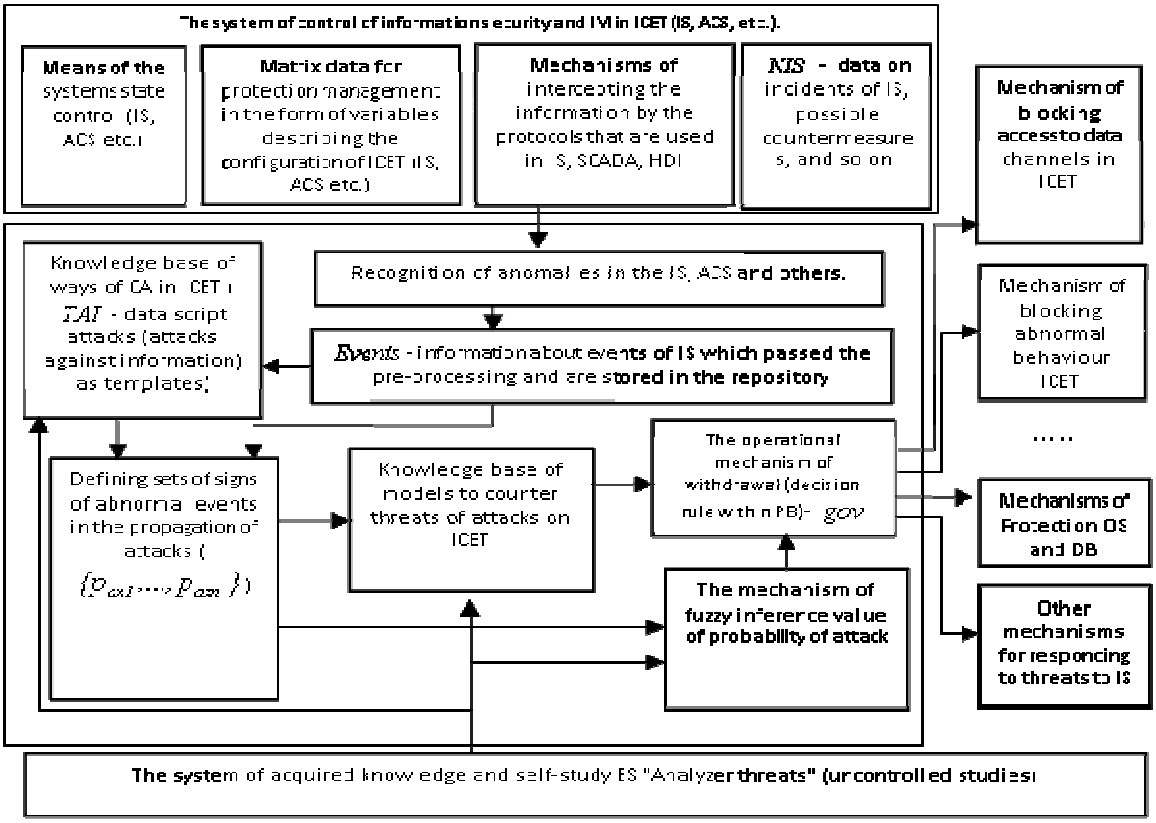

Fig. 4. The Structure Of Modules Of Intelligent Recognition System Threats (Uncontrolled Studies)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ES is designed to: threats recognition of ICET TS; obtain information about the state of the computers in the LAN; scans running programs and processes; determine the levels of security server and workstation; assessment of current risks unauthorized access to IS and ACS.

5. RESULTS

Examples of test results for DPTI information security of ICET TS were shown on Fig. 5, 6.

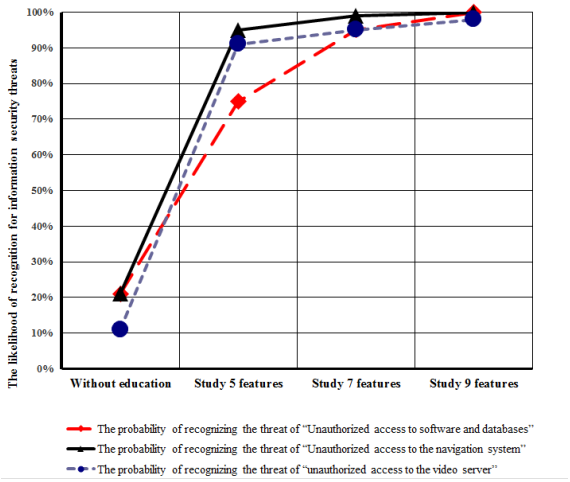

Fig. 5. The probability of threats detection (TD) of typical attacks on the information in ICET

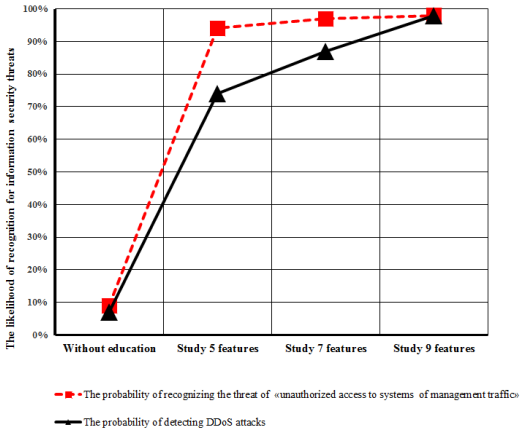

Fig. 6. The probability of TD of typical attacks on the information in ACS

In the task of attacks recognition on information in ICET a number of attributes has a weight close to zero, but there are many such values that have quite a lot of weight, that is very typical for one of the classes.

During the tests were used representative sets of limited length. The maximum length of the feature of set class of attacks on information resources IS or ACS was equal to 3. In a smaller maximum length the most of the sites did not contain any representation set. An increase in the maximum length to 4 increases the time of the algorithm.

If you place the characteristics of class assault on IS or ACS in decreasing order of informativeness, it is generally allocated to each class group features with a large informative, followed by a break, and signs, that were left then, are being built in a line with gradually decreasing informativeness.

6. DISCUSSION

DPTI advantages are: receiving function classification with minimal error classification; an opportunity to use the linear of classifiers to work with non-linear data; ability to work with diverse complicated structured data; in case of changes in the structure of the analyzed data usually just enough to change $gov(p_{axi})$ without changing the algorithm DPTI.

For each class of threats make a study sample of 100-250 (sp_{an}) objects, divided into appropriate classes. For each class the number of attacks on information signs varied from 3 to 9. Informational characteristics changed in the range of -1 to +1. To assess the effectiveness of recognition procedures, use the method of sliding control.

7. CONCLUSION

The main research results are:

1. Studied the question of introduction of modern information and communication systems and technologies on transport. It was found that the complexity of the application for recognition of threats of formalized system of analysis and synthesis of ICET ISIS is that a particular set of information and its subsystem IS containing disparate elements that describe using various mathematical models. It is shown that the use of adaptive elements of information security based on the use of new methods and models predictive threat detection of ICET.
2. Suggested the new recognition method based on discrete threats treatments using the device of logic functions and fuzzy sets that can increase the efficiency of recognition of ICET threats depending on the class to 85-98%.
3. It was developed the method of formation of the decision rule for discrete recognition procedures threats to information security, based on critical analysis of ICET procedure of individual elements, and allows you to perform threat detection with a minimal number of errors. It is shown that the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

construction of the set of elementary of classifiers for this class of threats reduced to the maximum permissible and conjunction for characteristic function of the class.

REFERENCES:

[1] Ahmad D., Dubrovskiy A., Flinn X. *Defense from the hackers of corporate networks*, DMK, Moscow 2005.

[2] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, *Basic concepts and taxonomy of dependable and secure computing, IEEE Trans.Dependable and Secure Computing*, USA 2004.

[3] John R. Vacca. *Managing Information Security*. Syngress – 2010. - 320 pp.

[4] William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin. *Firewalls and Internet Security*, 2nd Edition. Addison Wesley – 2003. - 464 pp.

[5] Korchenko O., Vasiliu Y., Gnatyuk S. *Modern quantum technologies of information security against cyber-terrorist attacks.* Aviation, 2010.

[6] *Transportation & Logistics 2030. Securing the supply,* Germany 2014.

[7] Industrial control systems and SCADA cyber security. – *Engineering & Technology*, August 2014.

[8] Xinyi Huang, Yang Xiang, Elisa Bertino, Jianying Zhou, and Li Xu. "Robust Multi-Factor Authentication for Fragile Communications". IEEE Transactions on Dependable and Secure Computing, to appear.

[9] Aldar Chan and Jianying Zhou. "Cyber-Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem". IEEE Journal on Selected Areas in Communications, July 2014.

[10] V. Lahno, A. Petrov. *Ensuring security of automated information systems, transportation companies with the intensification of traffic*, Ukraine 2011.

[11] Mirkovic J. Internet Denial of Service: Attack and Defense Mechanisms. / Mirkovic J., Dietrich S., Dittrich D., Reiher P. – Prentice Hall PTR, 2004. 400 p.

[12] K. Trivedi, D. Kim, A. Roy, *Dependability and Security Models. Department of Electrical and Computer Engineering Duke University Durham*, NC, USA 2001.

[13] *Worldwide Security and Vulnerability Management 2004-2014,* National Computer Center Publications, Manchester 2014. [14] D. Harel, *Visual Formalism for Complex Systems*, USA 1987, p. 231-274.

[15] F. Lau, S. Rubin, M. Smith, L. Trajkovic, *Distributed denial of service attack*s, USA 2000, p. 304.

[16] V. Lahno, A. Petrov, *Modelling of discrete recognition and information vulnerability search procedures,* TEKA, Poland 2010, p. 137-144.

[17] V. Lahno, A. Petrov, *Experimental studies of productivity change in corporate information systems for companies in terms of computer attacks*. *Information security,* Ukraine 2011.

[18] V. Lahno, A. *Petrov, Management and production engineering. Modeling information security system of transport enterprises,* Bielsko-Biala 2012.

[19] Y. Xiang, W. Zhou, M. Chowdhury, *A Survey of Active and Passive Defence Mechanisms against DDoS Attacks.* TR, Australia 2004.

[20] J. Mirkovic, S. Dietrich, D. Dittrich, P. Reiher, *Internet Denial of Service: Attack and Defense Mechanisms,* Prentice Hall PTR, UK 2004.

[21] C. Chapman, S. Ward, *Project Risk Management: processes, techniques and insights,* USA 2003.

[22] M. Atighetchi, P. Pal, F. Webber, *Adaptive Cyberdefense for Survival and Intrusion Tolerance,* Internet Computing, USA 2004.

[23] S.-D. Chi, J.S. Park, K.-C. Jung, J.-S Lee, *Network Security Modeling and Cyber At-tack Simulation Methodology*, LNCS, USA 2001.

[24] Chirillo J. *Hack Attacks Testing - How to Conduct Your Own Security Audit*, Wiley, USA 2003.

[25] V. Mehta, C. Bartzis, H. Zhu, E.M. Clarke, J.M. Wing, *Ranking Attack Graphs, Proceedings of Recent Advances in Intrusion Detection*, Hamburg, Germany, 2006.

[26] Shun-Chieh Lin, Shian-Shyong Tseng, *Constructing detection knowledge for DDoS intrusion tolerance. Expert Systems with Applications,* USA 2004.

[27] S. Templeton, K. Levit, *A Requires/Provides Model for Computer Attacks*. USA 2000.

[28] Kaufmann, A. and Gupta, M.M. Introduction to fuzzy arithmetic: Theory and Applications, Van Nostrand Reinhold, New York, 1991, 361 p.

[29] Zimmermann H.-J. Fuzzy Set Theory – and Its Applications, Kluwer Academic Publishers, Boston/Dordrecht/London, 1992, 399 p.