UDC 004.056.53:656.078

V.A. Lahno, A.S. Petrov, A.G. Korchenko

MODELS, METHODS AND INFORMATION TECHNOLOGIES OF PROTECTION OF INFORMATION SYSTEMS OF TRANSPORT BASED ON INTELLECTUAL IDENTIFICATION OF THREATS

In article results of researches on development of methods and models of intellectual recognition of threats to information systems of transport. The article to contain results of the researches, allowing to raise level of protection of the automated and intellectual information systems of the transportation enterprises (AISTE) in the conditions of an intensification of transportations. The article to contain mathematical models and results of an estimation information systems having Internet connection through various communication channels. The article also considers the issues of research and protection of the AISTE under the condition of several conflict data request threads.

Keywords: information security, information security, intelligent recognition of threats, logic functions, fuzzy sets, heterogeneous data streams, the transport industry.

Introduction

The influence of information automation systems pervades many aspects of everyday life in most parts of the world. In the shape of factory and process control systems, they enable high productivity in industrial production, transport systems they provide the backbone of technical civilization. One of the foremost transport businesses security concerns is the protection of critical information, both within their internal financial infrastructures and from external elements. Now more and more open and standardized Internet technologies (e-business, e-logistics, e-cargo etc.) are used for that purpose.

The focus on cyber security is increasing rapidly due to many high profile and highly disruptive/damaging security breaches threatening financial and physical damage across critical national and corporate infrastructures. It also appears the nature of the threat is changing[1].

The automated systems on transport vary in technologies applied, from basic management systems such as car navigation; traffic signal control systems; container management systems; variable message signs; automatic number plate recognition or speed cameras to monitor applications, such as security CCTV systems; and to more

[1] D.Ahmad, A. Dubrovskiy, X. Flinn, *Defense from the hackers of corporate networks,* Moscow 2005, p.170.

[2] A. Avizienis, J.-C. Laprie, B. Randell, C. Landwehr, *Basic concepts and taxonomy of dependable and secure*

advanced applications that integrate live data and feedback from a number of other sources, such as parking guidance and information systems; weather information; and the like.

A Transportation Management System (TMS) is a software system designed to manage transportation operations. TMS are one of the systems managing the supply chain. They belong to a sub-group called Supply chain execution (SCE). TMS, whether it is part of an Enterprise Level ERP System and has become a critical part of any (SCE).

The block diagram of a typical control system for transport, figure 1.

Rapidly changing external and internal business environment, necessity to adapt oneself very quickly and take adequate management decisions in time make the effective use of corporate information to be a pre-requisite for business success.

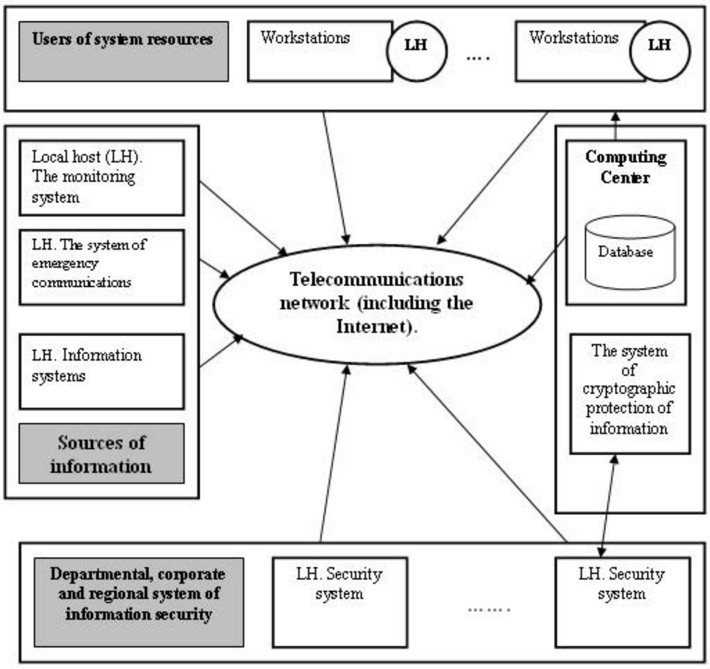

Users of system resources
Workstations
LH
....
Workstations
LH
Local host (LH). The monitoring system
LH. The system of emergency communications
LH. Information systems
Sources of information
Telecommunications network (including the Internet).
Computing Center
Database
The system of cryptographic protection of information
Departmental, corporate and regional system of information security
LH. Security system
....
LH. Security system

Fig. 1. The block diagram of control system for transport

Various functions of automated information management systems for transportation: Management of road, railway, air and maritime transport; Planning and optimizing of terrestrial transport rounds; Transportation mode and carrier selection;Real time vehicles tracking; Service quality control; Vehicle Load and Route optimization; Transport costs and scheme simulation; Shipment batching of orders; Cost control, KPI (Key performance indicators) reporting and statistics.

Since economic activities in Ukraine and CIS countries have boosted in the recent years and, therefore, nomenclature and volume of traffic has considerably grown, load on all types of transport (railway, motor, air, sea and pipeline transport) has been increasing. Along with increasing capacities of the existing and construction of new transportation capacities, there are great reserves in enhancing efficiency of the existing capacities (reduction of idle time due to more accurate planning, etc.) and organization of automated information exchange among consignors, carriers and other participants in the transportation process. Various forms of wireless communications technologies have been proposed for intelligent transportation systems in Europe, USA and Asia. Short-range communications (less than 500 yards) can be accomplished using IEEE 802.11 protocols. Theoretically, the range of these protocols can be extended using Mobile ad-hoc networks. Longer-range communications have been proposed using infrastructure networks such as IEEE 802.16, GSM, or 3G. Long-range communications using these methods are well established, but, unlike the short-range protocols, these methods require extensive and very expensive infrastructure deployment. There is lack of consensus as to what business model should support this infrastructure.

Today there is a wide range of software products of the leading vendors at the market (Interbase, Oracle, IBM, SAP, Sun Microsystems, Informatica), aimed at ensuring the maximum quality of resolving these tasks. Service-oriented architecture (SOA) and technologies of web-services based on open standards are very popular.

The modern approach to ensure the reliability of information processes (IP) and its protection from unauthorized access (UA) is supported at the international level by standard ISO/IEC 15408. According to this approach, a reliable IP successfully counteracts to the specified threats of security at the given external conditions of its operation. This leads to continuous improvement as ways and means of information protection (MIP) as well as ways and means of implementation of threats to information security (IS), resulting that appearance of new MIP leads to its bypassing by means of attack[2,3].

Information security management has become a critical and challenging business function because of reasons such as rising cost of security breaches, increasing scale, scope and sophistication of information security attacks, complexity of information technology (IT) environments, shortage of qualified security professionals, diverse security solutions from vendors, and compliance and regulatory obligations.

[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] K. Trivedi, D. Kim, A. Roy, *Dependability and Security Models*, USA 2001, p. 290.

As part of the state and interstate programs of information to create information systems, information-management and automated information systems transport industry (ISTI), as well as state integrated information system (SIIS).

Active expansion of information and communication environment in transport, accompanied by the emergence of new threats to information security (IS), as evidenced by the statistics of incidents (see Figure 2)[4].

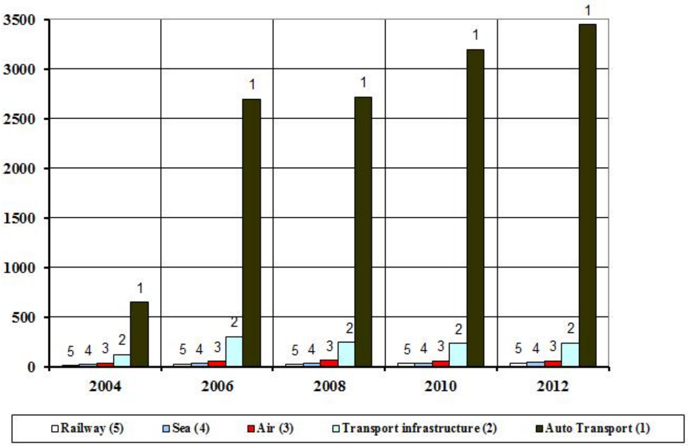


Fig. 2.The number of incidents of information security in transport

This, in its turn leads to the need for a new interpretation of the term "reliability of IP" that should be understand as lack of security vulnerabilities, which can be a consequence of the implementation of the various unintentional and intentional threats.

This eliminates a number of inconsistencies in the definition of conflict MIP and attack.

In so doing, the reliability of IP should be characterized by its conformity to some reference security model (invincible) circulation (processing and transmission) of information. In this regard, there is a practical problem that such things are only partially implemented in practice and is not directly reflected in the relevant standards for architectural solutions of automated systems, such as transport[5] satisfying the common reference models.

Studies on the further development of models and methods of information security based on the intelligent recognition of threats and information security in transport is one of the main problems of information protection of critical infrastructures state.

[4] *Transportation & Logistics 2030. Securing the supply,* Germany 2014. pp. 254-286.

[5] V. Lahno, A. Petrov. *Ensuring security of automated information systems, transportation companies with the intensification of traffic*, Ukraine 2011, p. 170.

The reason lies in the fundamental theoretical difficulties of modeling technologies ensuring the reliability and protection of IP in automated data processing systems of critical applications (ADPS CA) occurring when you try to connect a promising approach to ensure the safety and protection of IP from UA with the flexibility of the protective mechanisms.

The purpose of the article - description of the method and models of recognition of information security threats, which, unlike the existing permit to take a final decision on the existence of a threat to existing and new classes of attacks against information systems.

1. Previous researches

The results of researches, allowing raising the level of protection of the automated and intellectual information systems of motor transport (AIS) enterprises under conditions of transportations intensification are presented in the work.

The Top 10 information security threats for 2014:

1. Malware (Rising Threat).
2. Malicious Insiders (Rising Threat).
3. Exploited Vulnerabilities (Steady Threat).
4. Careless Employees (Steady Threat).
5. Mobile Devices (Rising Threat).
6. Social Networking (Rising Threat).
7. Social Engineering (Steady Threat).
8. Zero-Day Exploits (Rising Threat).
9. Cloud Computing Security Threats (Rising Threat).
10. Cyberespionage (Rising Threat).

The 2014 CVE survey found 90% of respondents detected computer security breaches within the last year and 73% reported financial losses due to these computer breaches. Questions about the adequacy of the Ukrainian science, engineering, and technology workforce are also rising to a chorus. Reported shortages of skilled workers in the IT sector are only one example.

To evaluate security of such a system, a security analyst needs to take into account the effects of interactions of local vulnerabilities and find global vulnerabilities introduced by interactions. This requires an appropriate modeling of the system. Important information such as the connectivity of elements in the system and security related attributes of each element need to be modeled so that analysis can be performed. Analysis of security vulnerabilities, the most likely attack path, probability of attack at various elements in the system, an overall security metric etc. is useful in improving the overall security and robustness of the system. Various aspects, which need to be considered while deciding on an appropriate model for representation and analysis, are: ease of modeling, scalability of computation, and utility of the performed analysis. The analysis of the protection of information systems and automated control systems for transport companies has yielded the following results (period 2012 -2014), fig. 3, 4[6].

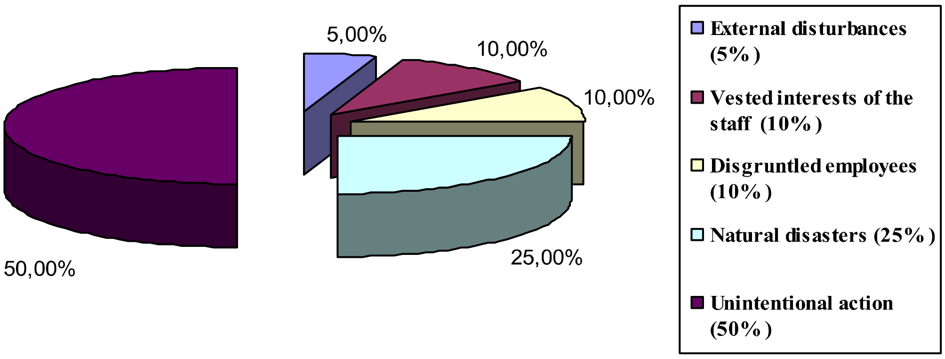


Fig. 3. The distribution of sources breach AIS

The decision of questions of complex maintenance of security and stability of functioning of the AIS in the conditions of unauthorized access (UNA), including, influences of computer attacks, demands the system analysis and synthesis of possible variants of construction of means of counteraction UNA means. At complex formation it is necessary to co-ordinate and inter connect functions and parameters of the EXPERT, protection frames of the information from UNA, anti-virus means, gateway screens, the communication equipment, the general and special software and perspective means of counteraction to computer attacks.

[6] *Worldwide Security and Vulnerability Management 2004-2014,* Manchester 2014, p. 178.

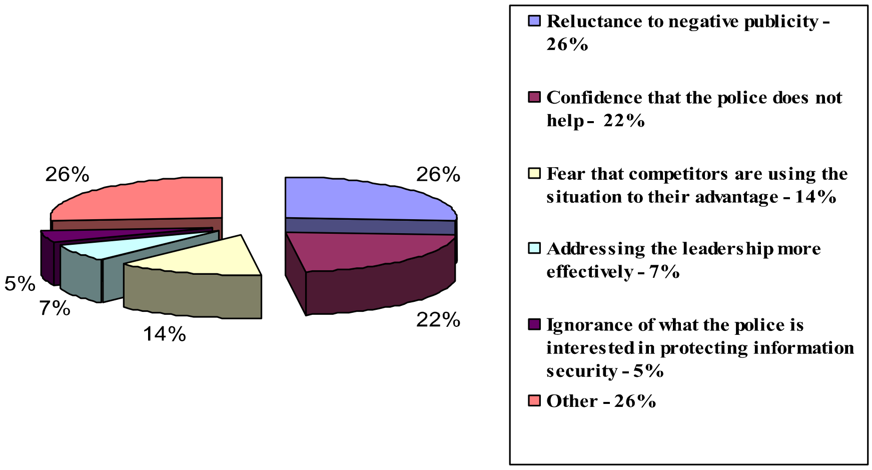


Fig. 4. The reasons for silence with information security incidents

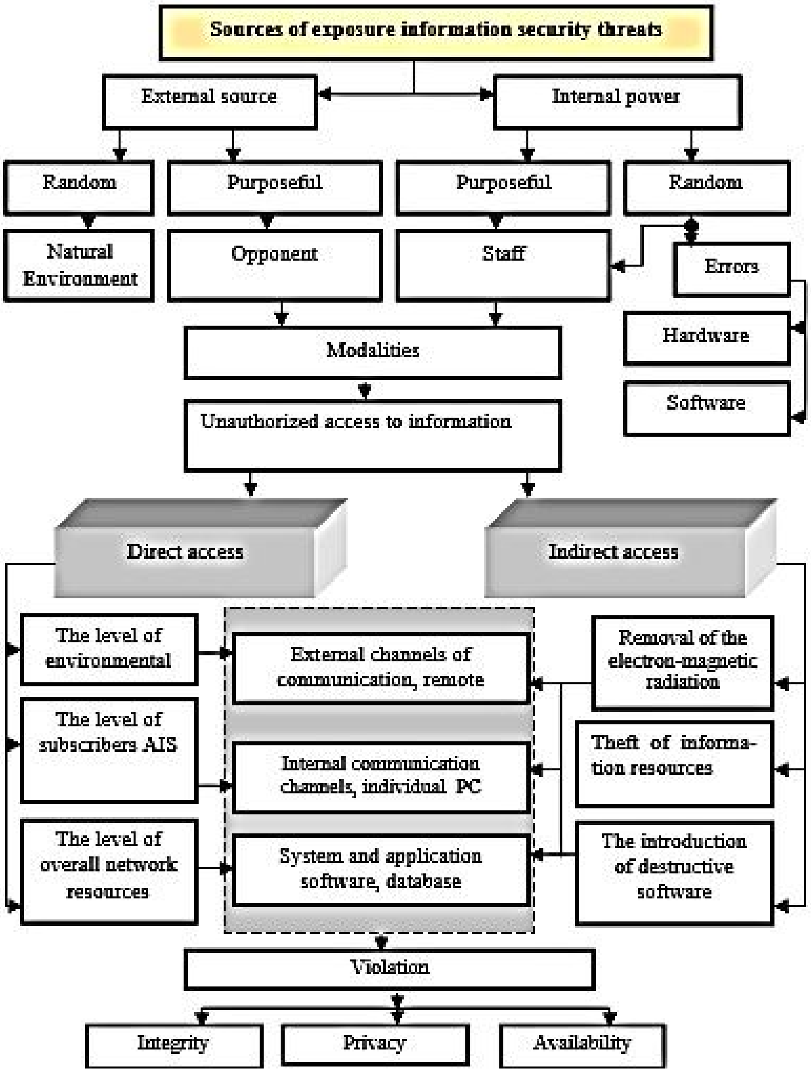

Sources of exposure information security threats
External source
Internal power
Random
Purposeful
Purposeful
Random
Natural Environment
Opponent
Staff
Errors
Hardware
Software
Modalities
Unauthorized access to information
Direct access
Indirect access
The level of environmental
The level of subscribers AIS
The level of overall network resources
External channels of communication, remote
Internal communication channels, individual PC
System and application software, database
Removal of the electron-magnetic radiation
Theft of information resources
The introduction of destructive software
Violation
Integrity
Privacy
Availability

Fig. 5. Sources of exposure information security threats

As a result of systematic analysis of relevant information security threats, figure 5. The classification has been done with certain basic features and gives an idea about the various options of a destructive impact on information resources.

Security professionals are aware that cyber criminals have increasingly sophisticated weapons at their disposal for maneuvering through online commerce systems and stealing information. Traditional firewalls, IPS/IDS, and web application firewalls do little to help online businesses understand the behavior of website visitors. Instead, they narrowly focus on the network and server exploits only. The challenge of detecting anomalous activity in real-time requires gathering various “big data” sources and correlating them to understand user behavior. However, current methods of detection fall short of this goal – individually, they examine only pieces of the behavior puzzle, not the entire picture[7,8].

To determine the likelihood of a future adverse event, threats to AIS must be analyzed in conjunction with the potential vulnerabilities and the controls in place for the AIS. Impact refers to the magnitude of harm that could be caused by a threat’s exercise of a vulnerability. The level of impact is governed by the potential cyberattacks impacts and in turn produces a relative value for the assets and resources affected (e.g., the criticality and sensitivity of the information system components and data).

Threat assessment system consists of the following steps:

1. System Characterization (AIS);
2. Threat Identification;
3. Identification vulnerability;
4. Control Analysis;
5. Likelihood Determination;
6. Impact Analysis;
7. Risk Determination;
8. Control Recommendations;
9. Results Documentation.

A threat is the potential for a particular threat-source to successfully exercise a specific vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited. A threat-source does not present a risk when there is no

[7] D. Harel, *Visual Formalism for Complex Systems*, USA 1987, p. 231-274.

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

vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities AIS, and existing controls.

The goal of second step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the information system being evaluated. A threat-source is defined as any circumstance or event with the potential to cause harm to an information system. The common threat sources can be natural, human, or environmental.

In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an automated information system and its processing environment. Result - a threat statement containing a list of threat-sources that could exploit system vulnerabilities.

The analysis of the threat to an automated information system must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources. Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system’s security policy.

2. Models, methods and information technologies of protection of corporate systems of transport based on intellectual identification of threats

The main task of discrete recognition and vulnerability search procedures (DRVSP) building is search of informative sub descriptions (or description fragments) of objects[9].

We consider informative objects to be the objects that reflect certain regularities in description of objects used for training, that is presence or, vice versa, absence of these fragments in the object, which is being considered, allows attributing it to one of classes. The fragments that are met in descriptions of one-class objects and cannot be met in descriptions of other classes’ objects are considered to informative in DRVSP. The regarded fragments as a rule have a substantial description in terms of designing information safety systems (ISS).

An elementary classifier is understood as a fragment in a description of a training sample. A certain multitude of elementary classifiers with preset properties are built for each $\{KL_1,..., KL_l\}$class. Another problem is presence of objects, which are on

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

borderline between classes $\{KL_1,..., KL_l\}$ and $\{B_{p_{a1}},..., B_{p_{al}}\}$among the study samples of objects. Each of such objects is not “typical” for its class, as it resembles to descriptions of objects belonging to other classes. Presence of untypical objects extends the length of fragments used to distinguish objects belonging to different classes. Long fragments are less frequent in new object, thus extending the number of unrecognized objects.

The necessity of building effective realizations for discrete recognition and vulnerability search procedures is directly connected to problems of metric (quantitative) characters of informative fragments’ multitudes. The most important and technically complex are the problems of obtaining asymptotical estimates for typical number values of (impasse) coveringand the length of integer matrix (impasse) covering and also the problems of obtaining analogical estimates for permissible and maximum conjunctions of a logical function, which are used for synthesis of circuit hardware-based ISS solutions.

There is, as a rule, no reliable information about the structure of *PA* multitude available while solving tasks connected with projecting an effective AIS information safety system, that’s why having built a discrete recognition and vulnerability search procedures algorithm we cannot guarantee its high performance on new objects different from $\{sp_{a1},..., sp_{am}\}$. Nevertheless, if the training samples are quite typical for the considered multitude of objects, than the algorithm that makes infrequent mistakes in studies will show acceptable results with unknown (not included in training samples) objects also. In this connection, correctness of discerning algorithm is the problem that should be paid great attention. The algorithm is considered to be correct if it discerns all the training samples correctly.

The main objective is to search DRVSP building fragments describing objects, see. Table 1.

The simplest example of a correct algorithm is the following: the considered object $sp_{an}$is compared to descriptions of every training sample$\{sp_{a1},..., sp_{am}\}$. In case if the sp_{an}object’s description coincides with a description of a sp_{an}training sample, the sp_{an}object is attributed to the same class as the sp_{ai} object. In other case, the algorithm declines to recognize the object. There is no difficulty noticing that though the foregoing algorithm is correct, it is not able to discern any object which description does not coincide with description of any training sample[10].

Let us introduce the following symbols. Let NP_{p_a} stand for a set of r_{p_a} , $r_{p_a} \le MI$ different integer-valued characters of $\{p_{aj_1},\dots, p_{aj_r}\}$ kind.

Thus, the schematic circuit of estimation algorithm building for information safety systems is the following. The whole range of different $NP_{p_a} = \{p_{aj_1},\dots, p_{a_M}\}$, $r_{p_a} \le MI$ type sub multitudes is picked out inside the $\{p_{a_1},\dots, p_{a_{jM}}\}$ character system. Later the picked sub multitudes are named reference multitudes of the algorithm, and their whole range is designated by ΩMI .

Further, let us set the following parameters:

- po_{sp_a} is a parameter characterizing significance of a sp_{ai}, *i= 1, 2,..., PA*target (object);
- $po_{NP_{pa}}$ is a parameter characterizing significance of an object belonging to a reference multitude $NP_{p_a} \in \Omega MI$.

Table 1

The knowledge base for the intelligent recognition of threats to information systems

Attributes (Signs Class threats)	Signs Class threats	The importance of sign	The univer-sum	Terms for the linguistic evaluation $\phi_u,\dots,\phi_v$
The set of classes of information security threats $KL = \{KL_1,\dots, KL_n\}$, The set targets for attack $PA = \{PA_1,\dots, PA_z\}$, The set of information security $N_j^{p_a} = \{n_1^{p_{a1}},\dots, n_j^{p_{au}}\}$, The mathematical sets of possible attackers $U = \{u_1,\dots, u_g\}$, The sets of incidents	$p_{ax} =$ $= \{p_{ax1},\dots, p_{ax_{MI}}\}$.	based on NIS $-1 \le IZ_{p_{axj}} \le 1$	$[0, N_{\grave{a}}]$ or [0,1], c. u.	Critical and uncritical *or* Identified, partially identified threats, undiagnosed

[10] V. Lahno, A. Petrov, *Experimental studies of productivity change in corporate information systems for companies in terms of computer attacks. Informationsecurity*, Ukraine 2011, p. 181-189.

$NIS = \{nis_1,..., nis_f\}$, The sets of variants attack on the system $AT = \{AT_1,..., AT_q\}$ and others.				
The state systems (AIS) $S_{IK} = \{S_{IK_1},..., S_{IK_m}\}$				
Methods and means of protection of information systems $D_{çç^3} = \{D_{çç^3_1}, ..., D_{çç^3_r}\}$				
The rules for result output *IF(*$KL_1 \vee ... \vee KL_n \vee S_{IK_J} \vee ... \vee S_{IK_m}$*) THEN*$D_{çç^3_r}$ and $\mu^{d_j}(S_{IK_i}) = \overset{h_j}{\underset{p=1}{\vee}}\left[\mu^{y_1}(y_1) \wedge ... \wedge \mu^{\phi_v}(\phi_v)\right]$, $p = \overline{1, h_j}, j = \overline{1, MI}$, де $\mu^{y_1}(y_1),..., \mu^{\phi}(\phi_u)$, $\mu^{\phi}(\phi_v)$ – membership function *y₁*, $\phi_u ,..., \phi_v$ of the fuzzy variables to terms; *y₁* – the state of information security {below critical, critical, above the critical, high}; $\vee$ – logical **OR**, $\wedge$ - Logical **AND** as operations max and min, respectively.				

Further comes the estimation procedure. The considered object $sp_{an}$is compared to every training sample sp_{ai} of every reference multitude.

A $\tilde{A}(sp_a, KL)$ estimation of sp_a object belonging to *KL* class is calculated for each vulnerability class of AIS KL, $KL \in \{KL_1,..., KL_l\}$ in the following way:

$$\tilde{A}(sp_a, KL) = \frac{1}{|LW_{KL}|}\sum_{sp_{ai}\in KL}\;\sum_{NP_{p_a}\in\Omega MI} po_{sp_a} \cdot po_{NP_{pa}} \cdot BN(sp_a, sp_{ai}, NP_{p_a}), \quad (1)$$

Where $|LW_{KL}| = |KL \cap \{sp_{a1},..., sp_{aMI.}\}|$.

The sp_{an}object is attributed to the class that has the highest estimate. In case if there are several classes with the highest estimate, discerning fails. Obviously, the ready-built algorithm is not always correct. Correctness of this algorithm requires compliance with a linear inequalities system of the following type:

$$\begin{array}{l} \tilde{A}(sp_{a1}, KL_1) > \tilde{A}(sp_{a1}, KL_2),\ \tilde{A}(sp_{aMI_1}, KL_1) > \\ > \tilde{A}(sp_{aMI_1}, KL_2),\ \tilde{A}(sp_{aMI_{1+1}}, KL_2) > \tilde{A}(sp_{aMI_{1+1}}, KL_1). \\ \cdot \quad \cdot \quad \cdot \\ \tilde{A}(sp_{aMI}, KL_2) > \tilde{A}(sp_{aMI}, KL_1). \end{array} \quad (2)$$

The solution of the system comes up to choice of $\mathrm{po}_{\mathrm{sp}_{\mathrm{ai}}}$ *i* = 1, 2,...,*PA,*and $\mathrm{po}_{\mathrm{NP}_{\mathrm{pa}}}$, $\mathrm{NP}_{\mathrm{p_a}} \in \Omega\mathrm{MI}$ parameters. In case if the system is not combined, its maximum combined subsystem should be found and the solution of this subsystem defines the parameter points for $\mathrm{po}_{\mathrm{sp}_{\mathrm{ai}}}$ and $\mathrm{po}_{\mathrm{NP}_{\mathrm{pa}}}$.

Let's regard the situation, when the objects of the considered PA multitude are described by the characters, each possessing values of the {0, 1,..., $\mathrm{k}_{\mathrm{p_a}}$ - *1*} multitude.

Let's associate the $(\sigma_{\mathrm{DOP}}, \mathrm{NP}_{\mathrm{pa}})$ elementary classifier,where $\sigma_{\mathrm{DOP}} = (\sigma_{\mathrm{DOP}_1}, \ldots, \sigma_{\mathrm{DOP}_r})$, $\mathrm{NP}_{\mathrm{pa}}$ is a set of characters numbered $\mathrm{j}_1, \ldots \mathrm{j}_{\mathrm{r_{pa}}}$, with an elementary conjunction $\mathfrak{R} = \mathrm{p}_{\mathrm{axj}_1}^{\sigma_{\mathrm{DOP1}}} \ldots \mathrm{p}_{\mathrm{axj}_{\mathrm{r_{pa}}}}^{\sigma_{\mathrm{DOPr_{pa}}}}$.

If $\mathrm{sp_a} = (\alpha\mathrm{p_{a1}}, \ldots, \alpha\mathrm{p_{aMI}})$ is an object of the *PA*multitude, then obviously $\mathrm{BN}(\sigma_{\mathrm{DOP}}, \mathrm{sp_a}, \mathrm{NP_{pa}}) = 1$ only in case when $(\alpha\mathrm{p_{a1}}, \ldots, \alpha\mathrm{p_{aMI}}) \in \mathrm{NI}_{\mathfrak{R}}$, where $\mathrm{NI}_{\mathfrak{R}}$ is a truth interval for the elementary conjunction $\mathfrak{R}$.

Let's show that building a multitude of $(\mathrm{KL}_\mathrm{l}) = (\mathrm{B}_{\mathrm{p_{al}}})$ class elementary classifiers for the models previously considered in the article adds up to finding permissible and maximum conjunctions of the characteristic $(\mathrm{KL}_\mathrm{l}) = (\mathrm{B}_{\mathrm{p_{al}}})$ class function, which is a double-valued logical function possessing different values for training samples of KL_l *&* $\overline{\mathrm{KL}_\mathrm{l}}$.

The procedure of threat recognition for a certain target, that is the $\mathrm{sp_a} = (\alpha\mathrm{p_{a1}}, \ldots, \alpha\mathrm{p_{aMI}})$ object, is carried out based on the calculation built with the help of elementary conjunctions. Using the algorithm of conjunction calculation by class coverings seems to be the most economical in this case. A characteristic function of *KL₁* class of information threats is a certain logical function $\mathrm{F}_{\overline{\mathrm{KL}}}$, possessing value 0 for descriptions of $\mathrm{sp_{an}} = (\alpha\mathrm{p_{an1}}, \ldots, \alpha\mathrm{p_{anMI}})$ belonging to KL_l and possessing value 1 for other character sets belonging to $\mathrm{E}_{\mathrm{KL}}^{\mathrm{MI}}$. Here $\mathrm{E}_{\mathrm{KL}}^{\mathrm{MI}}$ is a multitude of all $\mathrm{r}_{\mathrm{p_a}}$ long sets. A permissible conjunction for $\mathrm{F}_{\overline{\mathrm{KL}}}$ is associated with the *KL₁* class covering, and the maximum conjunction for $\mathrm{F}_{\overline{\mathrm{KL}}}$ is associated with its terminal covering. A permissible (maximum) conjunction $\mathfrak{R}$ is used to determine if the $\mathrm{sp_{an}} = (\alpha\mathrm{p_{an1}}, \ldots, \alpha\mathrm{p_{anMI}})$ object belongs to $(\mathrm{KL}_\mathrm{l}) = (\mathrm{B}_{\mathrm{p_{al}}})$ class, in case if $(\alpha\mathrm{p_{a1}}, \ldots, \alpha\mathrm{p_{aMI}}) \notin \mathrm{NI}_{\mathfrak{R}}$.

Thus, building a multitude of elementary classifiers for the simulated class of information treats adds up to the following[11]:

1) specifying a characteristic function;

2) building a disjunctive normal form, which realizes this function. The biggest difficulty is building disjunctive normal forms from maximum conjunctions (shortened disjunctive normal forms) of a characteristic function;

3) calculating a permissible (maximum) conjunction $\Re$, which determines of the object belongs to a certain class of threats.

For each class, the number of threats to information security signs ranged from 3 to 9. Informational content of a sign can change in the range from -1 to +1. To evaluate the effectiveness of recognition procedures used cross-validation method. Examples of the results of performance testing method DRVSP shown in Fig. 6-9.

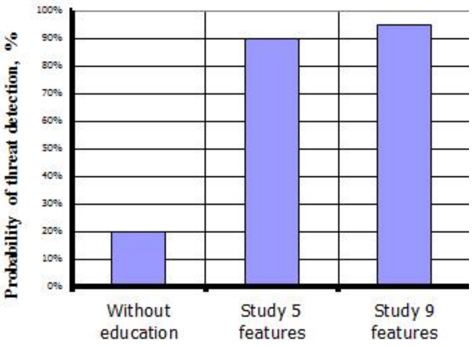


Fig. 6. The probability of recognizing the threat of "Unauthorized access to the video server"

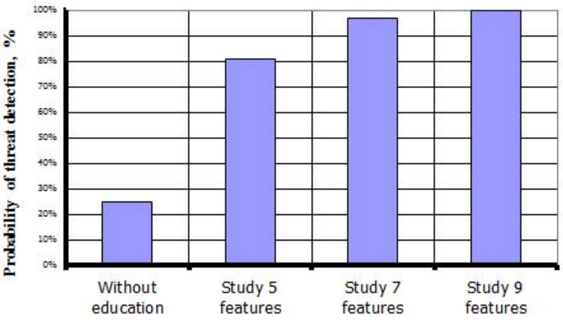


Fig. 7. The probability of recognizing the threat of "Unauthorized access to the user's password"

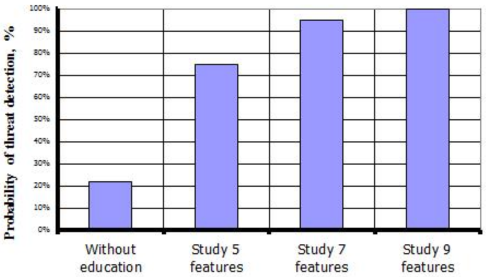


Fig. 8. The probability of recognizing the threat of "Unauthorized access to software and databases"

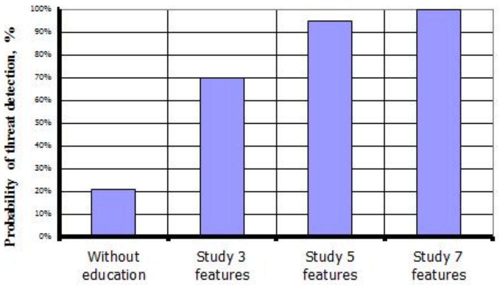


Fig. 9. The probability of recognizing the threat of "Unauthorized access to the navigation system"

In the following part of article the question of application of models of intellectual recognition of threats, for the task of the description of operation modes

[11] V. Lahno, A. Petrov,*Marketing and logistics problems in the management of organization. Task The Research of the conflict Request Threads in the Data Protection Systems,*Bielsko-Biala 2011, p. 230-251.

of information systems with blocking of the non-uniform flows of requests is considered. These non-uniform flows of requests meet in case of difficult invasions into information systems, for example, in modules of systems the client-bank, e-business, e-logistics, e-cargo, e-ticket, GSM-R, VSAT systems, etc.

During tests of the developed expert system (Fig. 10), the task of detection of DoS/DDoS of attacks is selected.

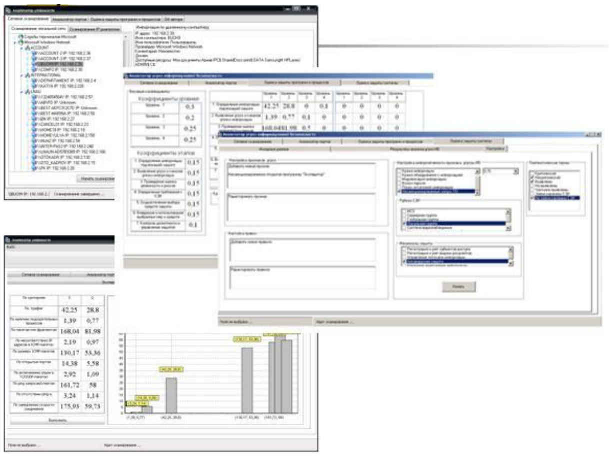
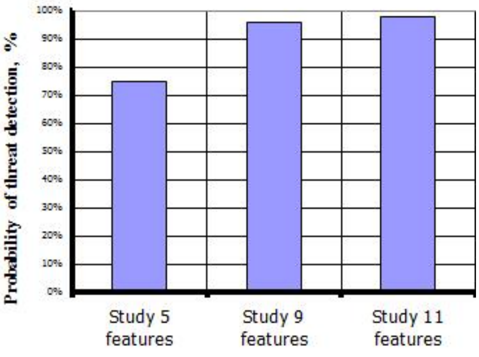


Fig. 10. General view of the "Analyzer threats"

The knowledge base from nine rules was used. The knowledge base is capable to define seven types of attacks of DoS/DdoS. In addition, known signs of attacks and additional signs for the description of a status of system (tab. 1) were used. Example list of factors that affect the productivity of information systems under the threat of DDoS attacks, presented in the form of linguistic variables, for which the selected set and universal terms. According constructed fuzzy knowledge base, representing a set of fuzzy rules "IF-THEN" that define the relationship between input and output variables. For fuzzy knowledge bases composed logical equation[12].



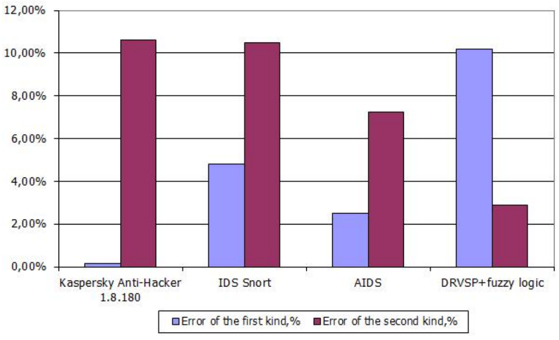


Fig. 11. Probability of detecting DDoS

Fig. 12. The value of error detection of

[12] V. Lahno, A. Petrov,*Management and production engineering. Modeling information security system of transport enterprises,* Bielsko-Biala 2012, p. 221-248.

attacks DDoS attacks of the first kind and the second kind

According to the results of the experiment, the DRVSP DoS/DDoS - attacks, following results were obtained for the errors of the first kind (false positives) - 10.2% for the error of the second kind (the number of detected attacks) - 2.9%, Fig. 12.

The discrete recognition search procedures allow creating "intelligent" system in which the detectors can effectively detect not only known but also unknown cyber-attacks. The structure, functioning and learning algorithms of discrete recognition search procedures detectors are presented. The results of studies that prove the effectiveness of the proposed approach are also presented.

3. Results

In the aftermath of the DDoS attacks, security experts identified network intrusion detection as one of several technologies that can lead to improved network security. While intrusion detection processes alone cannot prevent or defend against security attacks, they can serve as a valuable source of information for security administrators about the types of activity attackers may be using against them. Network intrusion detection (NID) is the process of identifying network activity that can lead to the compromise of a security policy.

With the fuzzy input sets defined, the security administrator can then construct the rules of the fuzzy system. Fuzzy rules are written using common sense experiences by the security administrator. The rules designer seeks to define rules that cover as much of the input space as possible Using tools such as the Matlab Fuzzy Toolbox, the designer can check the input rule space to ensure that the fuzzy rules cover the input space and that all output responses are defined, figure 13.

4. Conclusions of the work

Operation is devoted to research and development of theoretical methods, models and software products for support of information security on transport.

Main results of researches:

1) The method of intellectual recognition of threats based on the logic functions and indistinct sets has been developed. The method allows increasing the efficiency of recognition of threats for information security to 85-98% (depending on a threat class). In addition, it is possible, to use a method for creation of new systems of information security on transport.

2) The offered models have been realized in the form of expert system, which can increase efficiency of recognition of computer invasions DDoS to 97-98%.

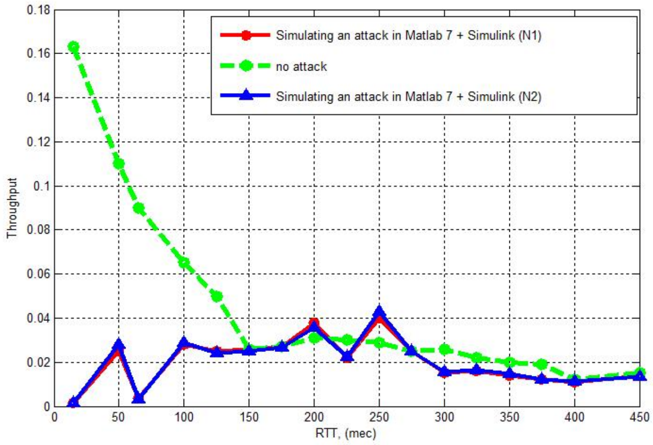


Fig. 13.Dos Inter-burst Period

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. K. Trivedi, D. Kim, A. Roy, Dependability and Security Models. Department of Electrical and Computer Engineering Duke University Durham, NC, USA 2001.
4. Transportation & Logistics 2030. Securing the supply, Germany 2014.
5. V. Lahno, A. Petrov. Ensuring security of automated information systems, transportation companies with the intensification of traffic, Ukraine 2011.
6. Worldwide Security and Vulnerability Management 2004-2014, National Computer Center Publications, Manchester 2014.
7. D. Harel, Visual Formalism for Complex Systems, USA 1987, p. 231-274.
8. F. Lau, S. Rubin, M. Smith, L. Trajkovic, Distributed denial of service attacks, USA 2000, p. 304.
9. V. Lahno, A. Petrov, Modelling of discrete recognition and information vulnerability search procedures, TEKA, Poland 2010, p. 137-144.
10. V. Lahno, A. Petrov, Experimental studies of productivity change in corporate information systems for companies in terms of computer attacks. Informationsecurity,Ukraine 2011.
11. V. Lahno, A. Petrov, Marketing and logistics problems in the management of organization. Task The Research of the conflict Request Threads in the Data Protection Systems,Bielsko-Biala 2011.

12. V. Lahno, A. Petrov, Management and production engineering. Modeling information security system of transport enterprises, Bielsko-Biala 2012.
13. Y. Xiang, W. Zhou, M. Chowdhury, A Survey of Active and Passive Defence Mechanisms against DDoS Attacks. TR, Australia 2004.
14. J. Mirkovic, S. Dietrich, D. Dittrich, P. Reiher, Internet Denial of Service: Attack and Defense Mechanisms, Prentice Hall PTR, UK 2004.
15. C. Chapman, S. Ward, Project Risk Management: processes, techniques and insights, USA 2003.
16. M. Atighetchi, P. Pal, F. Webber, Adaptive Cyberdefense for Survival and Intrusion Tolerance, Internet Computing, USA 2004.
17. S.-D. Chi, J.S. Park, K.-C. Jung, J.-S Lee, Network Security Modeling and Cyber At-tack Simulation Methodology, LNCS, USA 2001.
18. Chirillo J. Hack Attacks Testing - How to Conduct Your Own Security Audit, Wiley, USA 2003.
19. 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.