Decision Making in Manufacturing and Services
Vol. 9 • 2015 • No. 2 • pp. 117–136

Models, Methods and Information Technologies of Protection of Corporate Systems of Transport Based on Intellectual Identification of Threats

Alexander Petrov*, Valeriy Lakhno**, Alexander Korchenko***

Abstract. In the article, results of the research on the development of methods and models of intellectual recognition of threats to information systems of transport. The article contains results of the research that allows us to raise the level of protection of the automated and intellectual information systems of the transportation enterprises (AISTE) in the conditions of the intensification of transportation. The article contains mathematical models and results of 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: systems of transportation and communication, information security, cyber security, information security, threat detection, mathematical models, fuzzy logic

Mathematics Subject Classification: 94D05

Revised: October 26, 2015

1. 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 and transport systems, essentially providing the backbone of technical civilization. One of the foremost transport business 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 the many high-profile and highly disruptive/damaging security breaches that threaten financial and physical damage across critical national and corporate infrastructures. It also appears that the nature of the threat is changing (Ahmad *et al.*, 2005, p. 170).

* AGH University of Science and Technology, Krakow, Poland, e-mail: opietrov@zarz.agh.edu.pl, corresponding author
** European University, Kyiv, Ukraine
*** The National Aviation University, Kyiv, Ukraine

DOI: http://dx.doi.org/10.7494/dmms.2015.9.2.117

The automated systems on transportation vary in the technologies applied, from basic management systems such as car navigation, traffic signal control systems, container management systems, variable message signs, automatic number plate recognition, and speed cameras to monitoring applications such as security CCTV systems, and to more-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 is 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, has become a critical part of any (SCE).

The block diagram of a typical control system for transportation can be seen in Figure 1.

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

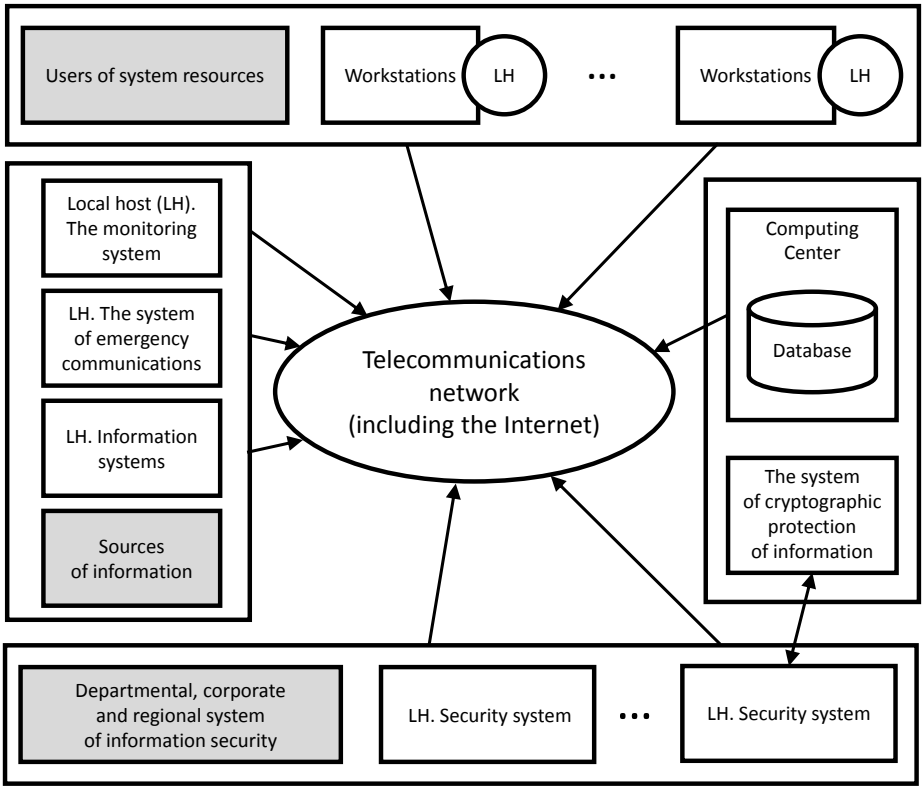

Fig. 1. *The block diagram of a control system for transport*
Source: own elaboration based on Lakhno and Petrov, 2011a, p. 8

Various functions of automated information management systems for transportation:

- management of road, railway, air, and maritime transport;
- planning and optimizing terrestrial transport rounds;
- transportation mode and carrier selection;
- real-time vehicle 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 increased in recent years, the subsequent, nomenclature and volume of traffic has grown considerably, causing, the load on all types of transportation (railway, motor, air, sea, and pipeline transport) to increase. Along with the increasing capacities of the existing infrastructure as well as the construction of new transportation capacities, there are great reserves in enhancing the 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 communication technologies have been proposed for intelligent transportation systems in Europe, the 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 which business model should support this infrastructure.

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

The modern approach of ensuring the reliability of information processes (IP) as well as 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 any specified threats of security at the given external conditions of its operation. This leads to continuous improvement, as the ways and means of information protection (MIP) as well as the ways and means of implementation of threats to information security (IS), resulting that the appearance of a new MIP leads to its bypassing by means of attack (Avizienis *et al.*, 2004; Trivedi *et al.* 2001, p. 290).

Information security management has become a critical and challenging business function due to reasons such as the 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.

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

The active expansion of the information and communication environment in transport, accompanied by the emergence of new threats to information security (IS), are evidenced by the statistics of incidents (see Figure 2) (*Transportation & Logistics 2030...*, 2014, pp. 254–286).

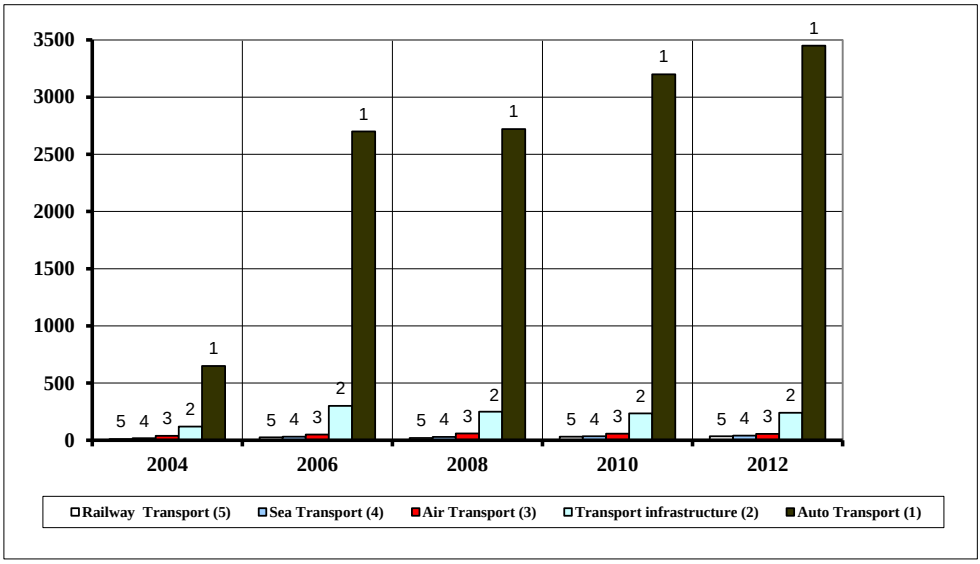

Fig. 2. *The number of incidents of information security in transport*

This, in turn, leads to the need for a new interpretation of the term "reliability of IP" that should be understood as a 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 (Lakhno and Petrov, 2011a, p. 170) 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 the critical infrastructure state.

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 is to provide a description of the method and models of recognizing information security threats that (unlike the existing systems) permits us to take a final decision on the existence of a threat to existing and new classes of attacks against information systems.

2. PREVIOUS RESEARCH

The results of research allowing us to raise the level of protection of the automated and intellectual information systems of motor transport (AIS) enterprises under conditions of transportation 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 that 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 the 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 interaction. 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, needs to be modeled so that analyses can be performed. The analysis of security vulnerabilities, the most likely attack path, probability of attack at various elements in the system, an overall security metric, etc., are useful in improving the overall security and robustness of the system. Various aspects that 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) (Figs 3 and 4) (*Worldwide Security...*, 2014, p. 178).

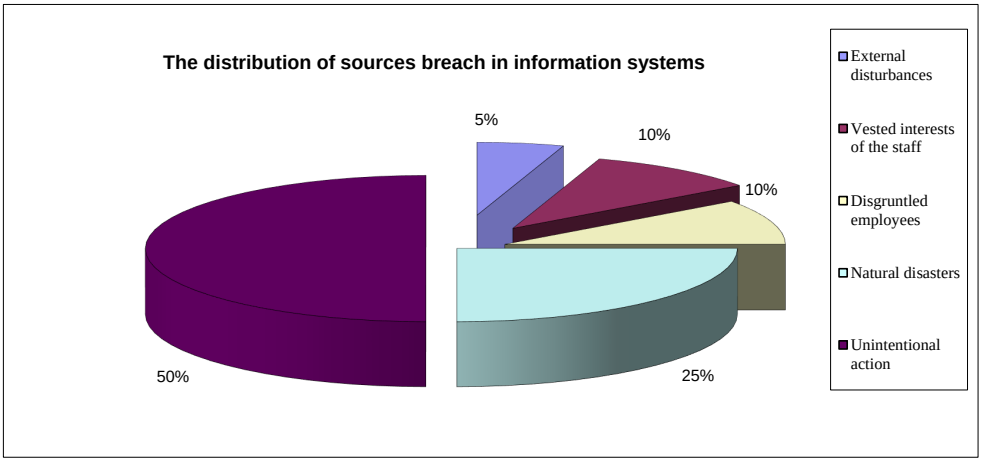

Fig. 3. *The distribution of source breach AIS*

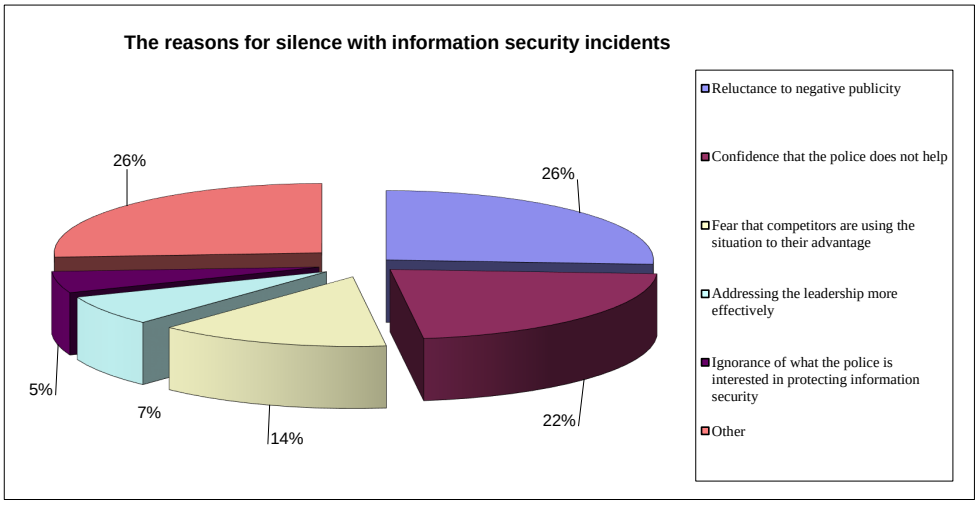

Fig. 4. *The reasons for silence with information security incidents*

The decision of questions of the 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 interconnect the functions and parameters of the EXPERT, protection frames of the information from UNA, anti-virus means, gateway screens, communication equipment, general and special software, and perspective means of counteraction to computer attacks.

As a result of the 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.

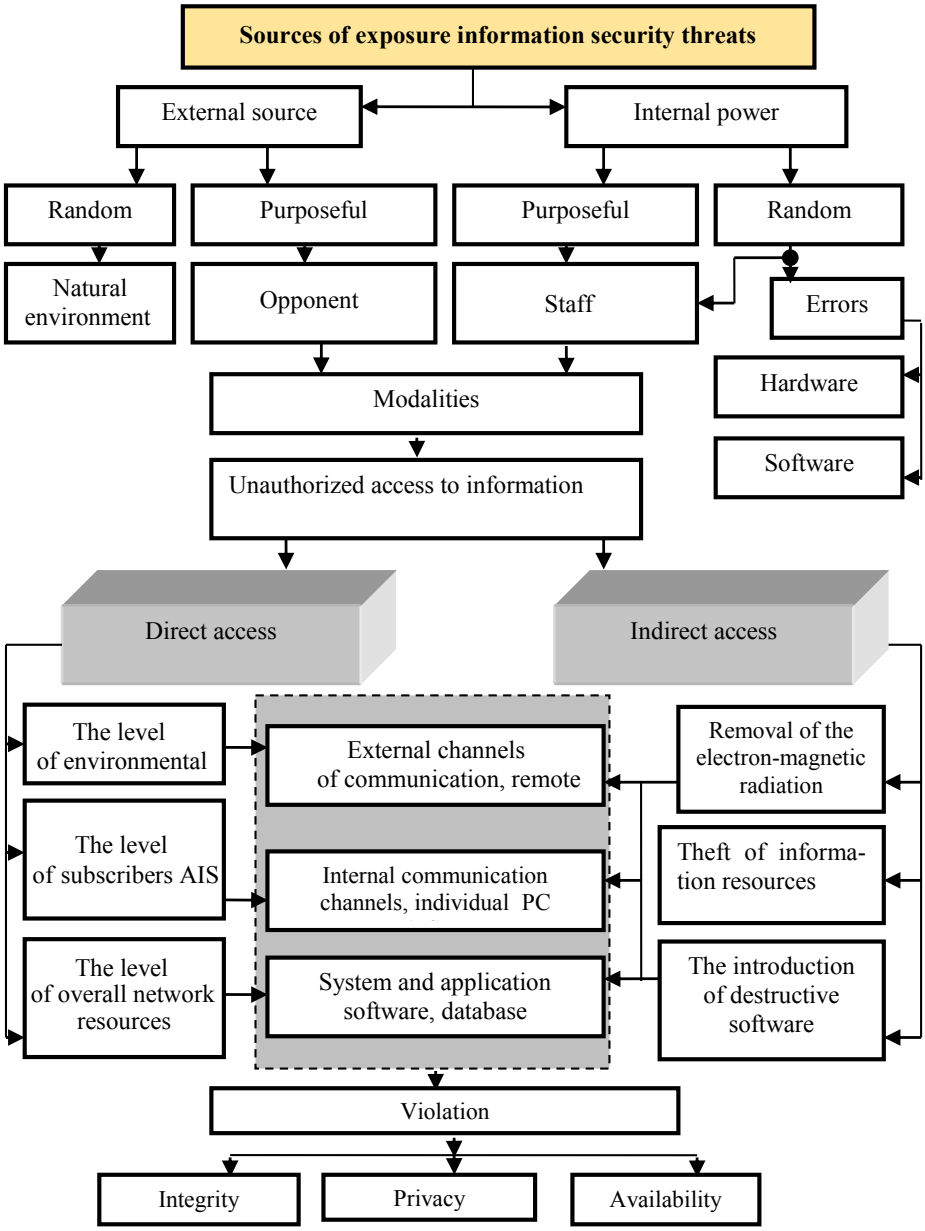

Fig. 5. *Sources of exposure information security threats*
Source: own elaboration based on Lakhno and Petrov, 2011a, p. 20

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 (Harel, 1987; Lau *et al.*, 2000).

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 particular vulnerability. The level of impact is governed by the potential cyberattack 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) result 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 vulnerability that can be exercised. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities of AIS, and existing controls.

The goal of the 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.

3. 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 procedure (DRVSP) building is to search of informative sub-descriptions (or description fragments) of objects (Lakhno and Petrov, 2010).

We consider informative objects to be those that reflect certain regularities in the description of objects used for training; that is, the presence or (vice versa) absence of these fragments in the object that is being considered, allowin us to attribute it to one of several classes. The fragments that are met in the descriptions of one-class objects and cannot be met in the descriptions of other classes' objects are considered to be 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 the presence of objects that are on the borderline between classes $\{KL_1, ..., KL_l\}$ and $\{B_{p_{a_1}}, ..., B_{p_{a_l}}\}$ among the study samples of objects. Each of these objects is not "typical" for its class, as it resembles the descriptions of objects belonging to other classes. The presence of atypical objects extends the length of fragments used to distinguish objects belonging to different classes. Long fragments are less frequent in a 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 the informative fragments' multitudes. The most important and technically complex are the problems of obtaining asymptotical estimates for typical number values of (impasse) covering and 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 is why, having built a discrete recognition and vulnerability search procedure 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, then the algorithm that makes infrequent mistakes in studies will also show acceptable results with unknown objects (not included in training samples). In this connection, the correctness of the discerning algorithm is a problem to which 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).

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 universum**	**Terms for the linguistic evaluation** $\phi_u,\ldots,\phi_v$
The set of classes of information security threats $KL = \{KL_1, ..., KL_n\}$, The set targets for attack $PA = \{PA_1, ..., PA_z\}$, The set of information security $N_j^{Pa} = \left\{n_1^{pa1}, ..., n_j^{pau}\right\}$, The mathematical sets of possible attackers $U = \{u_1, ..., u_g\}$, The sets of incidents $NIS = \{nis_1, ..., nis_f\}$, The sets of variants attack on the system $AT = \{AT_1, ..., AT_q\}$ and others	$p_{ax} = \{p_{ax1}, ..., p_{axMI}\}$	based on NIS $-1 \leqslant IZ_{paxj} \leqslant 1$	$[0,\ N_0]$ or $[0, 1]$, c. u.	Critical and uncritical or Identified, partially identified threats, undiagnosed
The state systems (AIS) $S_{IK} = \{S_{IK_1}, ..., S_{IK_m}\}$				
Methods and means of protection of information systems $D_{77V} = \{D_{77V_1}, ..., D_{77V_r}\}$				
The rules for result output *IF* $(KL_1 \vee ... \vee KL_n \vee S_{IK_J} \vee ... \vee S_{IK_m})$ *THEN* D_{77V_r} and $\mu^{d_j}(S_{IK_i}) = \overset{h_j}{\underset{p=1}{\vee}} \left[\mu^{y_1}(y_1) \wedge ... \wedge \mu^{\Phi_v}(\phi_v)\right]$, $p = \overline{1,\ h_j}, j = \overline{1,\ MI}$, where $\mu^{y_1}(y_1),\ldots,\ \mu^{\Phi}(\phi_u)$, $\mu^{\Phi}(\phi_v)$ – membership function y_1 , $\phi_u,\ldots,\phi_v$ of the fuzzy variables to terms; y_1 – the state of information security {below critical, critical, above the critical, high}; $\vee$ – logical **OR**, $\wedge$ – logical **AND** as operations max and min, respectively				

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 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 cases, 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 that the description does not coincide with description of any training sample (Lakhno and Petrov, 2011b, pp. 181–189).

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

Thus, the schematic circuit of the estimation algorithm building for information safety systems is as follows: the whole range of different $\mathrm{NP_{p_a}} = \{\mathrm{p_{aj_1}}, ..., \mathrm{p_{a_{MI}}}\}$, $r_{p_a} \leqslant MI$ type sub multitudes is picked out inside the $\{\mathrm{p_{a_1}}, ..., \mathrm{p_{a_{jMI}}}\}$ 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:

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

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

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

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

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

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

$$\begin{aligned} &\Gamma(\mathrm{sp_{a1}}, KL_1) > \Gamma(\mathrm{sp_{a1}}, KL_2),\ \Gamma(\mathrm{sp_{aMI_1}}, KL_1) > \\ &> \Gamma(\mathrm{sp_{aMI_1}}, KL_2),\ \Gamma(\mathrm{sp_{aMI_{1+1}}}, KL_2) > \Gamma(\mathrm{sp_{aMI_{1+1}}}, KL_1) \\ &. \quad . \quad . \\ &\Gamma(\mathrm{sp_{aMI}}, KL_2) > \Gamma(\mathrm{sp_{aMI}}, KL_1) \end{aligned} \quad (2)$$

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

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

Let's associate the $(\sigma_{\mathrm{DOP}}, NP_{pa})$ elementary classifier, where $\sigma_{\mathrm{DOP}} = (\sigma_{\mathrm{DOP_1}}, ..., \sigma_{\mathrm{DOP_r}})$, NP_{pa} is a set of characters numbered $\mathrm{j_1}, ...j_{r_{pa}}$, with an elementary conjunction $\Re = p_{axj_1}^{\sigma_{DOP_1}} ... \, p_{axj_{r_{pa}}}^{\sigma_{DOP_{r_{pa}}}}$.

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

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

The procedure of threat recognition for a certain target [that is, the $\mathrm{sp_a} = (\alpha \mathrm{p_{a1}}, ..., \alpha \mathrm{p_{aMI}})$ 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 KL_1 class of information threats is a certain logical function $\mathrm{F}_{\overline{\mathrm{KL}}}$, possessing value 0 for descriptions of $\mathrm{sp_{an}} = (\alpha \mathrm{p_{an1}}, ..., \alpha \mathrm{p_{anMI}})$ belonging to KL_l and possessing value 1 for other character sets belonging to $\mathrm{E}^{\mathrm{MI}}_{\mathrm{KL}}$. Here, $\mathrm{E}^{\mathrm{MI}}_{\mathrm{KL}}$ is a multitude of all $\mathrm{r_{p_a}}$ long sets. A permissible conjunction for $\mathrm{F}_{\overline{\mathrm{KL}}}$ is associated with the KL_1 class covering, and the maximum conjunction for $\mathrm{F}_{\overline{\mathrm{KL}}}$ is associated with its terminal covering. A permissible (maximum) conjunction $\Re$ is used to determine if the $\mathrm{sp_{an}} = (\alpha \mathrm{p_{an1}}, ..., \alpha \mathrm{p_{anMI}})$ object belongs to $(KL_l) = (B_{p_{a_l}})$ class, in case $(\alpha \mathrm{p_{a1}}, ..., \alpha \mathrm{p_{aMI}}) \notin \mathrm{NI}_{\Re}$.

Thus, building a multitude of elementary classifiers for the simulated class of information treats adds up to the following Lakhno and Petrov, 2011c, pp. 230–251):

1) specifying a characteristic function;
2) building a disjunctive normal form that 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 the object that 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 are shown in Figures 6–9.

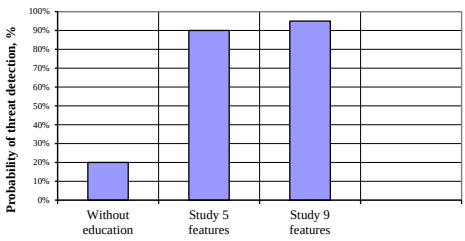

Fig. 6. *The probability of recognizing the threat of "unauthorized access to the video server"*

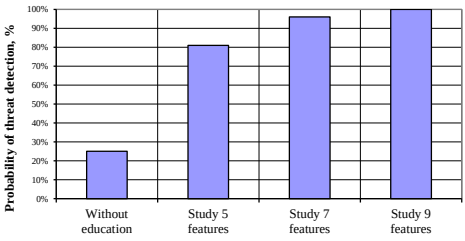

Fig. 7. *The probability of recognizing the threat of "unauthorized access to the user's password"*

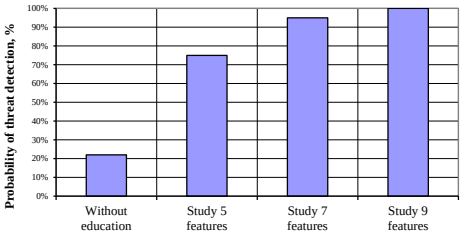

Fig. 8. *The probability of recognizing the threat of "Unauthorized access to software and databases"*

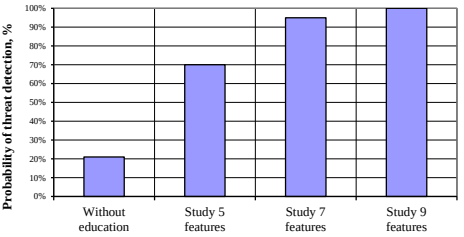

Fig. 9. *The probability of recognizing the threat of "Unauthorized access to the navigation system"*

In the following part of article, the question of which application of models of intellectual recognition of threats for the task of describing the operation modes 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 the modules of systems of client-bank, e-business, e-logistics, e-cargo, e-ticket, GSM-R, VSAT systems, etc.

During tests of the developed expert system, the task of detecting DoS/DDoS attacks is selected. The knowledge base from nine rules was used. The knowledge base is capable of defining seven types of attacks of DoS/DdoS. In addition, known signs of attacks and additional signs for the description of a status of system (Tables 1 and 2) were used.

Table 2. *Signs of a DoS/DDoS*

A partial state variable of the information system and Network	**Universum**	**Terms for linguistic assessment**
ϕ_1 – indicator of current risks [15–19]	[0,1], arbitrary units (A.U.).	*low*, *medium-low*, *medium*, *medium-high*, and *high*
ϕ_2 – acceptable level of risk information [20–22]	[0,1], A.U.	*critical and uncritical*
....	....	....
ϕ_{13} – presence of HTTP GET packets	[0,1], A.U.	*low*, *medium-low*, *medium*, *medium-high*, and *high*
ϕ_{14} – presence of HTTP flood packets	[0,1], A.U.	*low*, *medium-low*, *medium*, *medium-high*, and *high*
....	....	....
ϕ_z – other factors	[0,1], A.U.	*low*, *medium-low*, *medium*, *medium-high*, and *high*

The examples list 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 (Lakhno and Petrov, 2012, pp. 221–248).

For example, a system of logical equations for intelligent recognition of DDoS-attacks Application layer ("slow» HTTP GET flood and "slow» HTTP POST flood), we can write this:

$$\mu^{d_j}(S) = \bigvee_{p=1}^{h_j} \left[\mu^{y_1^{jp}}(y_1) \wedge \mu^{\phi_O^{jp}}(\phi_{13}) \wedge \mu^{\phi_O^{jp}}(\phi_{14}) \right], p = \overline{1,\ h_j}, j = \overline{1, M} \qquad (3)$$

where:

$\mu^{y_1^{jp}}(y_1)$, $\mu^{\phi_O^{jp}}(\phi_{13})$, $\mu^{\phi_O^{jp}}(\phi_{14})$ – membership function variables y_1, ϕ_{13}, ϕ_{14} their fuzzy terms y_1^{jp}, ϕ_{13}^{jp}, ϕ_{14}^{jp}, respectively,

S – the state protection of information systems against DoS/DDoS (Xiang *et al.*, 2004, pp. 15–17; Mirkovic *et al.*, 2004, p. 400),

y_1 – the state of information {below the critical (bc), critical (cr), above the critical (ac), high (h)} (Chapman and Ward, 2003, p. 390; Atighetchi *et al.*, 2004, pp. 25–33; Chi *et al.*, 2001, p. 290),

$\vee$ – logical OR, $\wedge$ – logical AND, like max and min, respectively.

Figure 10 shows the main results obtained during the test simulation recognition DoS/Ddos attacks.

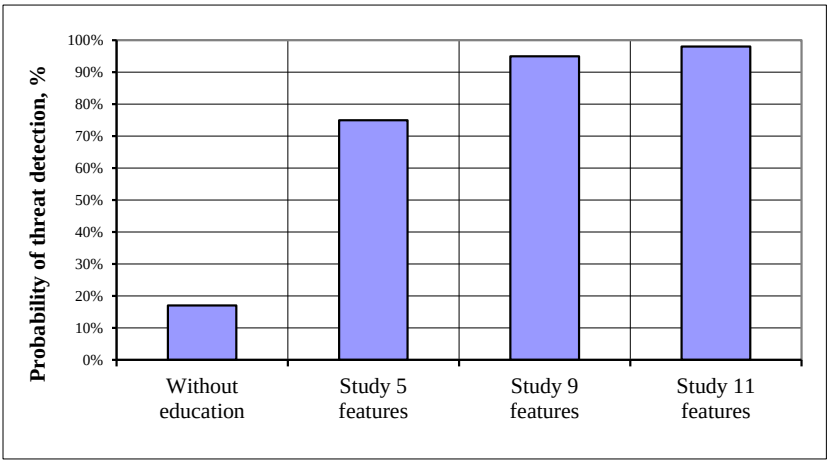

Fig. 10. *Probability of detecting DDoS attacks*

According to the results of the experiment, the DRVSP DoS/DDoS attacks, the following results were obtained: for the errors of the first kind (false positives) – 10.2%; for the errors of the second kind (the number of detected attacks) – 2.9% (Fig. 11).

The discrete recognition search procedures allow us to create an "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 procedure detectors are presented. The results of the studies that prove the effectiveness of the proposed approach are also presented.

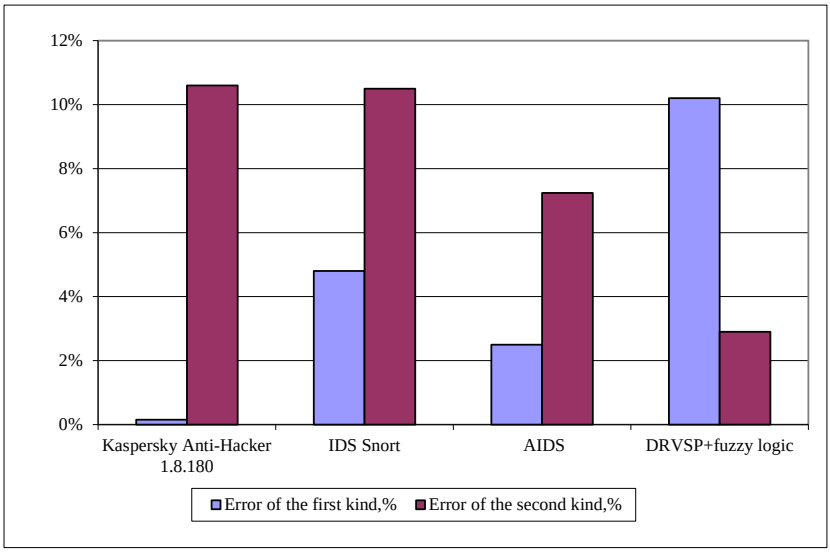

Fig. 11. *The value of error detection of DDos attacks of the first and second kinds*

4. 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 rule 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 (Fig. 12).

The successful attack on the AIS (particularly of type denial of service) does not necessarily require generating lots of server requests or decreasing bandwidth. A high degree of success probability can be reached by using the brittleness connected with the generation of a low-intensity priority thread; for example, by varying such parameters as packet speed (low-rate DoS attacks), quantity of packets with the zero rate as related to RTT, pulse length, etc.

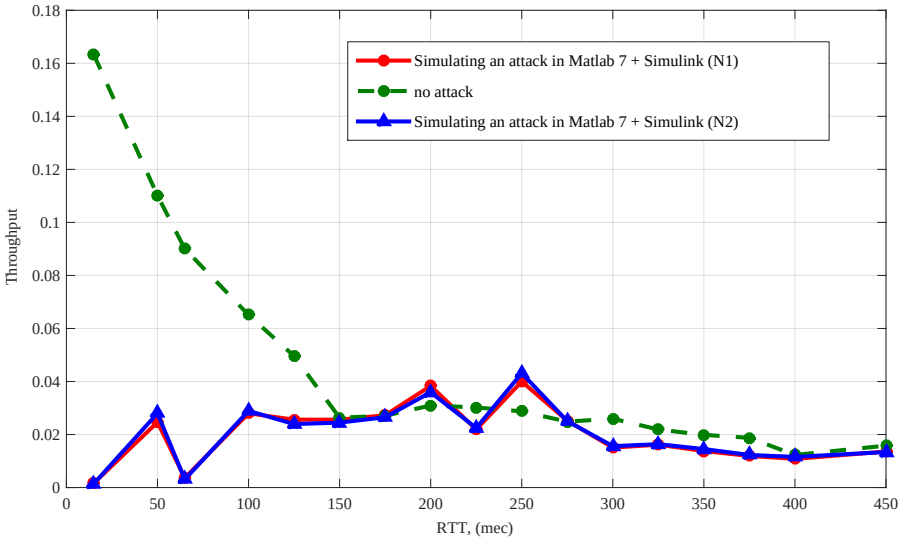

Fig. 12. *Dos Inter-burst Period*

The research has allowed us to develop the following sequence of IPM modeling stages in AISTE structure:

- to make a scheme of a multiphase queuing system (USYS) for the calculation of IPM capacious and time characteristics with use of MATLAB 2009 + Simulink;
- to execute the formalization of all possible states of the model system. To determine unsafe states;
- to determine the intensity and probability of the IPM transition from one state to another;
- to determine the characteristics of AISTE states as time and intensity functions of entering streams of requirements according to a transition graph, taking into account the differential or recurrent equations systems.

We have implemented the graphs attack in a combination of Prolog and Delphi (Fig. 13). Experimental results show that our logical attack graph tool is very efficient and can handle networks with thousands of machines.

We show screenshots of a few examples of Network Attack Graphs. States in the graph have been ranked according to the ranking algorithm based on PageRank. We set the damping factor to 0.85. For each error state, the intensity of color is proportional to the relative rank of that state in the Attack Graph.

The security metric based on the total rank of error states is a quantitative guide for comparing Attack Graphs. A system administrator could fix a particular security property, making changes to his network configuration and comparing the Attack Graphs obtained using this security metric. Thus, he can determine the relative utility of different security measures. He could also fix the system model and observe changes in the ranks of the Attack Graph based on varying the security property from a weak to a strong one. For example, consider the computer network shown in Figure 12, which

has interconnected computer hosts with some services and software vulnerabilities on each host. The total rank of error states in the changed Attack Graph is 0.045, which shows that the network becomes relatively more secure. Now, suppose the administrator also changes the security property to "Intruder cannot get root access on *ip1*".

Figure 14 shows the Attack Graph of the network with respect to the changed security property. The total rank of error states in the Attack Graph is 0.29. This shows that host ip1 is more likely to be attacked than host *ip2* in the changed network configuration.

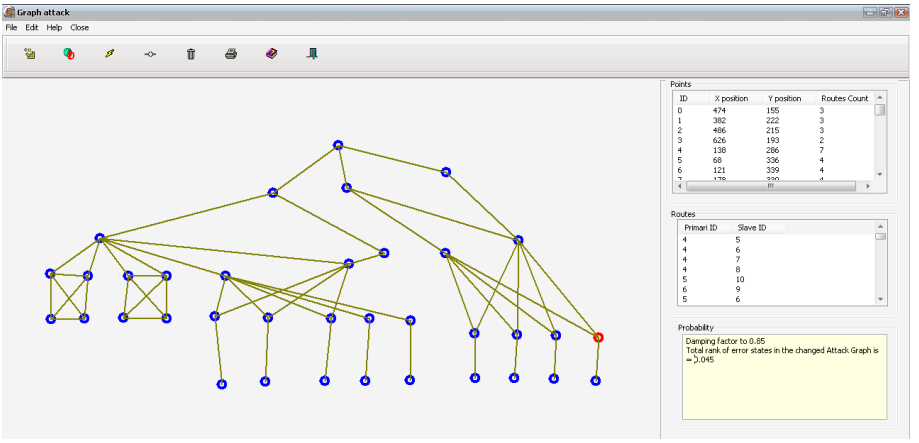

Fig. 13. *Comparison in Delphi Network Attack Graphs*

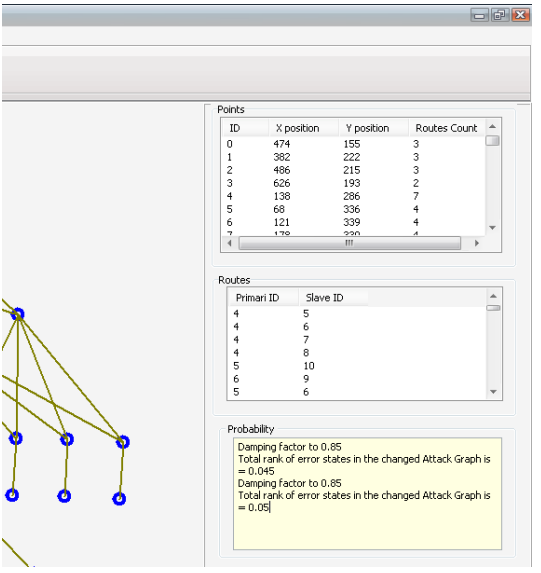

Fig. 14. *Comparison in Delphi Network Attack Graphs*

5. CONCLUSIONS OF THE WORK

The operation is devoted to research and development of theoretical methods, models, and software products for support of information security on transportation.

The main results of our research:

1) The method of intellectual recognition of threats based on the logic functions and indistinct sets has been developed. The method allows us to increase the efficiency of recognizing threats for information security to 85–98% (depending on the threat class). In addition, it is possible, to use a method for creating new systems of information security on transportation.
2) The offered models have been realized in the form of an expert system, which can increase the efficiency of recognizing computer invasions DDoS to 97–98%.

REFERENCES

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

Atighetchi, M., Pal, P., Webber, F., Schantz, R., Jones, Ch., Loyall, J., 2004, Adaptive Cyberdefense for Survival and Intrusion Tolerance, *IEEE Internet Computing*, **8**(6), pp. 25–33.

Avizienis, A., Laprie, J.-C., Randell, B., Landwehr, C., 2004. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, **1**(1), pp. 11–33.

Chapman, C., Ward, S., 2003. *Project risk management: processes, techniques and insights*, Wiley.

Chi, S.-D., Park, J.S., Jung, K.-C., Lee, J.-S., 2001. Network Security Modeling and Cyber At-tack Simulation Methodology. In: *Proceedings of 6th Australasian conference* (*Lecture Notes in Computer Science*, vol. 2119), Springer, pp. 320–333.

Chirillo, J., 2003. *Hack Attacks Testing – How to Conduct Your Own Security Audit.* Wiley.

Harel, D., 1987. Visual Formalism for Complex Systems. *Science of Computer Programming*, **8**(3), pp. 231–274.

Kolodgy, C.J., 2014. *Worldwide Security and Vulnerability Management 2004–2014.* National Computer Center Publications, Manchester.

Lakhno, V., Petrov, A., 2011a. Modelling of discrete recognition and information vulnerability search procedures. *Teka Komisji Motoryzacji i Energetyki Rolnictwa*, 11A, pp. 129–136.

Lakhno, V. Petrov, A., 2011b. *Ensuring security of automated information systems, transportation companies with the intensification of traffic.* Skhidnoukrayins'kyy natsonal'nyy universytet imeni Volodymyra Dalya (The Volodymyr Dahl East Ukrainian National University), Lugansk.

Lakhno, V., Petrov, A., 2011c. *Experimental studies of productivity change in corporate information systems for companies in terms of computer attacks. Information security.* Visnik Skhidnoukrayins'koho natsional'noho universytetu imeni Volodymyra Dalya, 5, pp. 181–189.

Lakhno, V., Petrov, A., 2011d. *Task the Research of the Conflict Request Threads in the Data Protection Systems.* In: Howaniec, H., Waszkielewicz, W., (eds), Marketing and logistics problems in the management of organization. Wydawnictwo Akademii Techniczno-Humanistycznej, Bielsko-Biała, pp. 230–251.

Lakhno, V., Petrov, A., 2012. *Modeling information security system of transport enterprises.* In: Dudek, M., Howaniec, H., Waszkielewicz, W., (eds), Management and production engineering. Wydawnictwo Naukowe Akademii Techniczno-Humanistycznej, Bielsko-Biała, pp. 221–248.

Lau, F., Rubin, S., Smith, M., Trajkovic, L., 2000. Distributed denial of service attacks. In: *Proceedings of 2000 IEEE International Conference on Systems, Man, and Cybernetics*, pp. 2275–2280.

Lin, Sh.-Ch., Tseng, Sh.-Sh., 2004. Constructing detection knowledge for DDoS intrusion tolerance. *Expert Systems with Applications*, **27**(3), pp. 379–390.

Mehta, V., Bartzis, C., Zhu, H., Clarke, E.M., Wing, J.M., 2006. Ranking Attack Graphs. In: *Proceedings of 9th International Symposium on Recent Advances in Intrusion Detection*, RAID, Hamburg, Germany, Hamburg, 20–22 September, Springer, Berlin–Heidelberg, pp. 127–144.

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

PricewaterhouseCoopers (PwC), 2014, *Transportation & Logistics 2030. Vol. 4: Securing the supply.* Available at: `www.pwc.com/tl2030`.

Smirniy, M., Lakhno, V., Petrov, A., 2009. *The research of the conflict request threads in the data protection systems.* Visnik Skhidnoukrayins'koho natsional'noho universytetu imeni Volodymyra Dalya, **2**(20), p. 23–30.

Templeton, S., Levit, K., 2000. A Requires/Provides Model for Computer Attacks. In: *Proceedings of the workshop on New security paradigms (NSPW '00).* ACM, New York, NY, USA, pp. 31–38.

Trivedi, K.S., Kim, D.S., Roy, A., Medhi, D., 2009. Dependability and security models. In: *Proceedings of 7th International Workshop on Design of Reliable Communication Networks*, pp. 11–20.

Xiang, Y., Zhou, W., Chowdhury, M., 2004. *A Survey of Active and Passive Defense Mechanisms against DDoS Attacks.* Technical Report, TR C04/02, School of Information Technology, Deakin University, Australia.