ZN WSH Zarządzanie 2017 (3), s. 147-167

Oryginalny artykuł naukowy
Original Article

*Data wpływu/Received:*12.07.2017
Data recenzji/Accepted: 17.07.2017/26.07.2017
Data publikacji/Published: 29.09.2017

Źródła finansowania publikacji: środki własne Autorów

Authors' Contribution:
- (A) Study Design (projekt badania)
- (B) Data Collection (zbieranie danych)
- (C) Statistical Analysis (analiza statystyczna)
- (D) Data Interpretation (interpretacja danych)
- (E) Manuscript Preparation (redagowanie opracowania)
- (F) Literature Search (badania literaturowe)

DOI: 10.5604/01.3001.0010.6496

Professor Dr Valeriy Lakhno [A B D]
European University, Ukraine

Professor Dr. hab. Eng. Alexander Petrov [C D]
AGH University of Science and Technology Faculty of Management

PhD Inna Nagorna [D E F]
European University, Ukraine

DEVELOPMENT OF A SUPPORT SYSTEM FOR MANAGING THE CYBER PROTECTION OF AN INFORMATION OBJECT

ROZWÓJ SYSTEMU WSPARCIA DLA ZARZĄDZANIA CYBERBEZPIECZEŃSTWEM OBIEKTU

Abstract: The information is being discussed and its characteristics in the system of enterprise management. The model of operational management information and cyber security (CS) object forms a rational set of remedies based on morphological approach. Unlike existing solutions, the model prepared on the basis of intelligent decision support, a morphological matrix for each facility's perimeters of information protection, and can generate a set of options for remedies which take into account the compatibility of software and hardware. The choice of the optimal option set for that perimeter protection of information, implements an objective function that maximizes the ratio of the sum "security information" to the total rate "cost."

Keywords: decision support system, information safety, information security management

Streszczenie: W artykule omówione zostały informacje i ich cechy charakterystyczne w systemie zarządzania przedsiębiorstwem. Model zarządzania operacyjnego informacji i przedmiot cyberbezpieczeństwa (CS) tworzy racjonalny zestaw środków zaradczych na podstawie morfologicznego podejścia. W przeciwieństwie do istniejących rozwiązań model ten został opracowany na podstawie inteligentnego wsparcia decyzji, matrycy morfologicznej dla każdego obwodu ochrony informacji i może generować zestaw opcji środków zaradczych, które uwzględniają kompatybilność oprogramowania i sprzętu. Wybór optymalnej opcji dla ochrony obwodowej informacji realizuje obiektywną funkcję, która maksymalizuje stosunek sumy „informacji o bezpieczeństwie" do całkowitego kosztu.

Słowa kluczowe: system wsparcia decyzji, bezpieczeństwo informacji, zarządzanie bezpieczeństwem informacji

Introduction

It is impossible to imagine modern attitudes and perspectives of further information-communicative systems (ICS) development in different fields of human activity without the increased attention of questions regarding informational security (IS) and cybersecurity (CS) particularly because of the increasing number of cyber attacks (C-A) and the destructive influence on information objects (IO) or ICS. The rapid increase of incidents in the field of IS has shown that existing information security systems (ISS), which are built on the basis of known threats and emerging attacks, are not always effective in cases of new C-A's which are created against the widespread enterprise information system (EIS), automated control systems (ACS, or SCADA) in electronics, industry, transport, the banking system etc.

For the successful usage of modern ICS it is necessary not only to know how to manage all the functional resources but to create an effective information security management system (ISMS). As management objects – ISMS are difficult organizational-technical structures (OTS), which function in conditions of uncertainty. Effective management of such systems has to be based on innovative information technologies aided by decision support which considers both IS and CS.

One of the variants of this solution is the usage of a decision support system (DSS) in CS on the basis of intelligent information technologies (IIT). Research into improving existing and the development of new methods, models, algorithms and software (SW) for operational management of information protection (IP) in IO/ICS, particularly in conditions of uncertainty, inconsistency and lack of knowledge about ICS status becomes highly relevant.

Problem statement. Suppose that in the process of organizational and technical cyber security management of the IO/ICS, the protection methods rational sets model planning stage (information protection means) is considered as a process of sequential removal of uncertainty of information security systems (ISS) structure and composition. Thus, the planning of rational compatible software and hardware sets information protection means (IPM) is a consideration of alternatives *AL* (the number of alternative setup variants): $PL = SFS \to CS_{al}$, where *SFS* – a range of functional sub-systems for perimeter IO/ICS; *CS* - chosen setup IPM. Then the decision selection by the intelligent decision of information security operational management support system is regarded as forming a subset of the best options set $CS' \subseteq CS$. In the study, the problem of comparing sets of information protection means options is examined using morphological matrix sets in terms of "information security" in the perimeter of information security systems IO/ICS and "costs" for *l* functional subsystem ISS, which operate in conditions of uncertainty, inconsistency and lack of knowledge about the state of the object which is protected.

Goal of the research – developing a cyber-threats (C-T's) counterwork model using DSS, choosing rational variants of reactions on the occurrences in CS, and taking into account current operational IO data.

It is necessary to solve the following tasks to reach the goal of the research:

1. To develop a model of operational management (OM) of CS IO/ICS which allows us to increase IS management efficiency in conditions of information environment status uncertainty, and efficiency of the ISS rational structure planning process.

2. To develop the intelligent decision support system (IDSS) program of IO/ICS cyber-security (CS) management (CSM) and to investigate the efficiency of the offered model.

1. Information and its security in the system of enterprise management

In the conditions of economy informatization, information is the resource most needed especially in the process of management, in the process of decision-making process. The company is "dumped" with a huge amount of information, much of which is redundant. While a large amount of information is very difficult to formalize, encode, process. The head of the enterprise is constantly faced with excess or (and) a lack of

information, but what is more painful – with a stream of incorrect, false information. Therefore, an effective management system must have reliable information.

To manage business it is used the solving system, which is a symbiosis of the person making the decision (EDM) and the computing system. In it, EDM should develop a vector of control parameters. In it turn, the control parameters control the manufacturing directly and indirectly, through its effects on the technical and economic indicators (TEI). The parameter is a set of control signals to maintain a given level of TEI. In the process of control parameters formation, there are a number of poorly formalized circumstances, including the estimated value of TEI. These indicators often contradict each other; for example, when there is a fall of output – profitability is increasing. The decision maker should consider all TEI. However, to formalize the enterprise management process before it is ended is not yet possible. Still in relation to some indicators only qualitative approaches are applied. The mechanism of their definition is still not fully developed, and considering weak structuring of the control system is shown only in additional verification of the decisions taken by the Director and his Deputy.

It should be noted that in the system of enterprise management accounting the factors of information lack does not have a pragmatic expressions, as the cost for creating a mathematical model to calculate it significantly exceed the reduction of losses due to considering this factor. In this regard we present only the formulas, which can perform calculations in the case if it will be necessary to ensure information security of the enterprise.

The value of information is determined by the formula:

$$C_u = log\ P_1 - log\ P_0 = log\ (P_1/P_0),\ (1)$$

where C_u – the value of the information.

This formula can be interpreted as follows: if P - the probability of achieving the goal – before receiving the information was equal to P_0, and after receiving - P_1, we can use the above formula.

It is necessary to consider not only the quantitative characteristics of information, but also semantic. For this purpose, and for action to eliminate the influence of the uncertainty factor, are used:

1. Syntax, according to which the equation of uncertainty of *H*. Shannan is applied:

$$H = -\sum_{i=1}^{n} p(A^3) \log_2 P(Ai)\ .\ (2)$$

This formula calculates the degree of uncertainty, and then determined the level of awareness, taking the optimum decisions:

$$Y = I / V_d\ ,\ (3)$$

where Y - the level of decision awareness; I - the quantity of information; V_d - the amount of data that is relevant to the decision made.

2. Semantic, according to which it is determined content of information:

$$S = I_c / V_d, \quad (4)$$

where S - informative information; V_d - amount of information that is perceived by the Manager.

3. Pragmatic: the value of the message to the decision-making process, frequency of implementation of management functions for a fixed period of time, the degree of influence of the communication on the accuracy of decisions, the economic effect from implementation in the system of management decision-making process.

The risk of information security breach in the enterprise management system is a situational characteristic of any enterprise activity, reflecting uncertainty of its outcome and possible negative consequences. For risk assessment it is used the three methods described below, which depend on a particular enterprise[1].

The first one: is required for "brave" projects they break the structure of production and provide a significant breakthrough in the market. For such projects, the risk is associated with the danger of incorrectly assessing the situation, whereby the sales will occur unsatisfactory. Therefore, when using such projects it is required continuous development of all possible alternatives to solve this task in order to compare their likelihood of implementation and to make the best decisions at any given moment of the enterprise activity[1].

The second method: used when there is a special variety of alternative solutions, but the project itself is quite complex that covers the entire product of life cycle from design to mass production. In this case, it is important to evaluate the reliability of each phase of the production process, identify the least reliable parts of the enterprise in order to develop them for activities that reduce risk, and thus to provide a certain level of economic security. Since the implementation of the project covers several quite distinct stages, it is advisable to carry out a risk assessment for each[1].

The third method: is applied in a relatively simple project and involves a more complex calculation due to the use of not just average values, and the nature of the distribution of those random variables whose average value used in the calculations. The most that you can count for is to estimate the distribution of a random variable and make a statistical modeling process[1].

When proving the information security in the enterprise we must strive to have the optimal control. Under the optimal control is understood a control, which together with imposed on a system constraints provides the extreme value of the efficiency

[1] I.P. Bosak & Ie. M. Palyha, *Informatsiine zabezpechennia upravlinnia pidpryiemstvom: ekonomichnyi aspect*, "Rehionalna ekonomika" 2007, Vol. 4, pp. 17–22.

criterion (maximum or minimum depending on the specific choice of the objective function). Therefore, it is necessary to achieve information security with the greatest efficiency in the neutralization of negative external impacts, at the same time the economic-mathematical model (EMM) has to have an optimization character.

The EMM that has optimization character includes: objective function whose value is minimized or maximized; the system of equations determining the dependence between all variables in the problem; the set of constraints that defines the boundaries of the values of variables in the problem.

Economy-mathematical modeling, that has optimization character has the following general form[2]:

$$Å = \sum Ci \cdot Xi \rightarrow Extr \text{ , (5)}$$

under the following restrictions:

$$\begin{cases} \sum aij \cdot Xi \{=<;=;>=\} bj, (j = \overline{(1,m)} \\ dj <= Xi <= Di, (i = \overline{(1,m)}, \end{cases} \text{ , (6)}$$

where *E* - the objective function; *Ci* - coefficients of the variables in the objective function; *Xi* - the variables of problem; *bj* - the right parts of restrictions; *aij* - coefficients of the variables in the constraints; *dj* - minimum possible values of the variables; *Di* - maximum possible values of the variables.

If all variables X, which are part of the equation fall into place in the first degree, the tasks are solved by such models are called linear programming problems.

To improve the efficiency of enterprise management system and ensure its information security, the management of the enterprise should determine which steps in the planning can be done if the scenario would be different. In the process of entering specific information it needs to be specified and the response, the ultimate goal of which must be either the C-T's or opportunities which appeared. As in case of external factors, the effects of internal factors on the performance of the region or state as a whole can be positive or negative. The objective conditions of existence are such that in the economic system of our country is nothing, but elements and relationships between them. To replace each item that is the subject or object (product, service), and replaced any connection between the elements, the company must react. In this formulation, the question of the reaction of the enterprise management system must be conformed to the following principles[3],[4].

[2] R. Kaliuzhnyi, M. Shvets, V. Shamrai, R. Kaliuzhnoho, V. Shamraia, *Informatsiine zabezpechennia upravlinskoi diialnosti v umovakh informatyzatsii: orhanizatsiino-pravovi pytannia teorii i praktyky,* Kiyv, 2002, pp. 56–61.

[3] H.A. Koposov, Y.Y. Nahornaia, *Pryntsypy ekonomycheskoi bezopasnosty predpryiatyia,* II Mizhnarodnoi naukovoi konferentsii, Cherkasy 2005, pp. 98–103.

[4] T.P. Tkachuk, *Formuvannia systemy informatsiinoi bezpeky biznesu,* "Biznes i bezpeka" 2009, Vol. 4, pp. 89–90.

1. The principle of comparative advantage. All economic parameters of the enterprise should not necessarily be optimal, but certainly better than any other company in this market. The market economy organized in such a way, the market eliminates the weak ones, so to survive in the market it's enough to exceed the economic parameters of most businesses.

2. The principle of current benefits. All economic parameters of the enterprise should be relatively best at any period of time, no matter what value was this. Enterprises in the information economy are always working in the condition of extreme shortage of time, so for survival it is not enough to prevail for an indefinite period of time, more over of the remote one, because the moment can pass or never occur. To survive you must take advantage at any time.

3. The principle of actual liquidity. The amount of the company obligations to all cooperating entities must be less than the amount of liabilities to the enterprise at any period of time, no matter what value was this. For the enterprise it may be the situation – products are competitive, the optimal volume of production, profit is stable, but it is on the verge of bankruptcy, since the amount of current payments significantly exceeds the amount of its current revenues. In such a situation it is difficult to explain to the creditors that you have the ability to pay in the future, especially when the creditor is interested to buy your company for a pittance, taking advantage of a temporary insolvency.

4. The principle of conformity. Any action of an enterprise in any market that falls within the scope of activity of the enterprise, must meet the requirements of society. The market economy created in such a way that it has the right for existence anything that increases individual effectiveness, but it remains only that improves public efficiency. For this reason, any action of the enterprise that harms social efficiency will sooner or later be punished. Or the entrepreneur produced the products of wrong quality or in the wrong amount, did the extra costs – punishment will be held for sure.

5. The principle of necessary and sufficient armament. The enterprise should have all you need for an adequate response to any action (internal or external), provided the minimum value of the reserves. To ensure security, there is an attractive way to stockpile on all occasions. However, this method is, firstly, impossible, due to the small size of personal capital, and, secondly, economically feasible, since the storage of excess funds in reserves, as we know, reduces the efficiency of capital. Thus, stocks should be, but these stocks should not "sink" the company.

6. The principle of market power possession. The company must have at least one advantage that can significantly reduce their own costs. The possession of market power always gives you the opportunity to influence the parameters of the market and get more profit, so the pursuit of market power is natural. However, the market of perfect competition, by definition, denies the existence of market power of any of the sellers. The only thing that can influence the manufacturer in this market, as at its

own costs. Producers have different skills, different experience, different relationships, different talents, and therefore are obliged to use their benefits to reduce costs.

7. The principle of leadership. The enterprise must constantly improve its activities ahead of the competition. A high degree of mobility of capital in a competitive market does not allow long to keep any advantage, so survival requires continuous innovation, including those that destroy the enterprise over a long period of time. In the latter case, the desire of competitors to repeat the experience will lead them to ruin.

8. The principle of sufficient awareness. The company must have reliable and timely information about upcoming changes in the external environment. One of the most significant market failures is asymmetry of information, where the lack of quality information leads to irrational actions that are harmful to public and individual effectiveness. The desire to obtain all necessary information is justified, but expensive. For this reason, it is better to have partial information as in case of occurrence of undesirable events – insurance.

9. The principle of mimicry. The company should organize its activities so as to remain unnoticed in the market. The company needs constantly hide their results and their true intentions; otherwise it will become an attractive target for attackers.

10. The principle of timely coagulation. Working on a given market while retaining its position (without improvements), the company is obliged to seek the moment out of this market. The invariance of positions in the market suggests that a portion of the above adheres to the principles of life, and the part cannot accurately implement. In this case, it is necessary to withdraw from the market, preserving capital, and to try to realize themselves in any other market.

Thus, the use of the apparatus of economic-mathematical methods and the theory of uncertainty, which allow consideration of all the available factors of influence on the work of the enterprise, is necessary for the development of enterprise management[5]. Revealed characteristics of information are used partly by modern authors to calculate information security. Only a systematic approach to business management and security on it will provide an opportunity to improve the results of the decisions to a qualitatively new level, which will promote the efficiency of enterprise management.

There is one main problem creating the CS – development of the threat model, which is connected to the specification of a management object interaction – ISS IO with the environment[6,7,8]. IDSS, which develops a threat model building method, is

[5] V.S. Tsymbaliuk, *Informatsiina bezpeka pidpryiemnytskoi diialnosti: vyznachennia sutnosti ta zmistu poniattia za umov vkhodzhennia Ukrainy do informatsiinoho suspilstva (hlobalni kibertsyvilizatsii),* "Pidpryiemnytstvo, hospodarstvo i parvo" 2007, Vol. 3, pp. 12–16.

[6] Y. Zhang, L. Wang, W. Sun, R.C. Green, M. Alam, *Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids*, "IEEE Transactions on Smart Grid" 2011, 2(4), pp.796–808.

[7] O. Al-Jarrah, A. Arafat *Network Intrusion Detection System using attack behavior classification*, "Information and Communication Systems (ICICS), 5th International Conference", 2014.

[8] P. Louvieris, N. Clewley, X. Liu, *Effects-based feature identification for network intrusion detection*, "Neurocomputing" 2013, 121(9), pp. 265-273.

based on a qualified scheme of goal-oriented destructive influences on IS and CS IO[9].

A generalized architecture of ISMS and CS is offered according to the results of the control strategy in conditions of uncertainty analysis[9].

Level of safety *(LS)* is used in the capacity of an operated variable. The *LS* value depends on the maximum level of information urgency which is being updated according to recent changes in ICS[9].

Mechanisms of IP control are created in the circuit with organizational-technical control (OTC) governing changing business applications, data array (DA) processing plans, infrastructure, and all the corresponding requests to the information safety level. The circuit contains: IDSS in regards to choosing a security strategy and a system of safety level assessment. Managing influence in the circuit is realized by the staff of the IS department. Command information is formed in the process of a goal-oriented choice of an information security method complex rational structure (ISMC).

Operational command information is formed in the CS and IS IO/ICS operational management (OM) circuit. This information is distributed to the management object by a security manager or automatically with the help of managing influences realization methods.

Effective solutions are chosen and decided according to the technical features of IP (ISM) as well as according to the IO/ICS controlled space status analysis.

The task of ISMC rational structure choice for IO is made according to the following criteria[10,11,12]: minimum probability of achieving goals by an attacker; minimum of IO losses should the attacker's goals be achieved; maximum probability of successful ISMC counteraction to the actions of an attacker; minimum "cost-risk" integrated index value.

Because of the fact that possible ICS topologies can be unequal for the offered ISMS architecture it is appropriate to use a model of a structural-technological reserve (STR) optimization for critically important DA and infrastructure components according to the criterion of minimum probability of a task solving impossibility[13].

---

[9] V. Lakhno, V. Malyukov, V. Domrachev, O. Stepanenko, O. Kramarov, *Development of a system for the detection of cyber attacks based on the clustering and formation of reference deviations of attributes*, „Eastern-European Journal of Enterprise Technologies" 2017, 3/9 (87), pp. 43-52.

[10] A. Fielder, E. Panaousis, P. Malacaria, C. Hankin, & F. Smeraldi, *Decision support approaches for cyber security investment*, "Decision Support Systems" 2016, Vol. 86, pp. 13–23.

[11] H. Cavusoglu, R. Srinivasan, T.Y. Wei, *Decision-theoretic and game-theoretic approaches to IT security investment*, "Journal of Management Information Systems" 2008, 25(2), pp. 281–304.

[12] Li-Yun Chang, Zne–Jung Lee, *Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system*, "International Conference on Fuzzy Theory and Its Applications" 2013.

[13] L. Atymtayeva, K. Kozhakhmet, G. Bortsova, *Building a Knowledge Base for Expert System in Information Security*, Chapter Soft Computing in Artificial Intelligence of the series Advances in "Intelligent Systems and Computing" 2014, Vol. 270.

So according to the task it is necessary to find such definitions $x_{nm}^{um^*}$,

$$\min_{\left\{X_{unum}^{um^*}\right\}} \prod_{un=1}^{N} \prod_{um=1}^{M_{\inf}} \left[\prod_{um^*}^{M_{\inf}} \varphi_{unum}^{um^*} \prod_{un'=1}^{N_{po}} \prod_{um'=1}^{M_{\inf}} \prod_{um_1^*=1}^{M_{\inf}^*} \prod_{um_2^*=1}^{M_{\inf}^*} P_{um_1^* um_2^*}^{unumun'um'} \right], \quad (7)$$

where *um* – a crosspoint in IO; M_{inf} – a quantity of DA; N_{po} – a program modules quantity; – φ_{unum}^{un} tasks allocation in IO crosspoints; – $P_{um_1^* um_2^*}^{unumun'}$ all the tasks in IO crosspoints solving probability;

limitations:

– for structural doubling of models $X_{unum}^{um_1^*} \; X_{un'um'}^{um_2^*} = 0$ for, $\forall un, um, un', um', um_1^*, um_2^*$, which for conditions are made $C_{um_1^* um_2^*} = 0$, $\varphi_{unum}^{un'um'} \neq 0$;

– for EIS, ACS, SCADA and other different modules allocation with different crosspoints $X_{unum}^{m^*} = 1$, for highlighted *unum* operational modules and um^*-*x* crosspoints;

– for the longest possible time of a task solving

$$\sum_{un=1}^{N_{po}} \max_{\left\{um^*\right\}} \left[X_{unum}^{um^*} \theta_{unum} \lambda_{unum} \right] + \sum_{un=1}^{N_{po}} \sum_{un'}^{N_{po}} \sum_{um=1}^{M_{\inf}} \sum_{um'=1}^{M_{\inf}} \max_{\left\{um_1^* \atop um_2^*\right\}} \left[X_{unum}^{um_1^*} X_{un'um'}^{um_2^*} \varphi_{unum}^{un'um'} \frac{1}{C_{um_1^* um_2^*}} \right] \leq T^* \quad (8)$$

where T^* – the longest possible time of a task solving; θ_{unum} – a requests quantity in EIS, ACS, SCADA and other; λ_{unum} – a task solving intensity; $\sum_{un=1}^{N_{po}} \sum_{um=1}^{M_{inf}} x_{unum}^{um^*} f_{unum} \leq V_{um^*}$. $\forall um^*, \; um^* = \overline{1, M_{inf}}$ – for maximum IO/ICS crosspoints secondary storage space

Using STR critical software and dataware (SW and DW) allows us to increase the safety level in conditions of destabilizing factors activity taking into account the longest possible task solving time limitation[14],[15].

Based on the analysis of ISMS potentially improving using new methods of task solving and the cycle time, improved efficiencies are offered by IDSS which allows us to rep-

[14] M. Kanatov, L. Atymtayeva, B. Yagaliyeva, *Expert systems for information security management and audit, Implementation phase issues*, Soft Computing and Intelligent Systems (SCIS), Joint 7th International Conference on and Advanced Intelligent Systems (ISIS), 2014.

[15] V. Lakhno, A. Petrov, *Ensuring security of automated information systems, transportation companies with the intensification of traffic*, Ukraine, 2011, pp. 154–176.

resent IP management mechanisms and to shorten operational information processing time.

2. Information object cyber-security operational management model

The safety level of *i*- IO/ISC crosspoint (EIS, ACS, SCADA and other) is determined by the following formula:

$$LS_i = 1 - IMI_{cis_i} = 1 - C_{ICR} \cdot At_i \cdot As_i \cdot TL_i \cdot LS_i \ , (9)$$

where IMI_{cis_i} – IS incident importance in *i*- IO/ISC crosspoint; At_i – IS breach level in *i*- IO/ISC crosspoint; As_i – data asset (DA) criticality in *i*- IO/ISC crosspoint; TL_i – trust level of a device, which reports about IS breaches in *i*- IO/ISC crosspoint; LS_i – security measures level in *i*- IO/ISC crosspoint; C_{ICR}=[0–1] – coefficient.

Quantity assessment of IO safety can be found the following way:

$$LS_{CIS} = \prod_{i=1}^{n} (1 - IMI_{cis_i}), \ (10)$$

where *n* – quantity of crosspoints in IO structure.

Quantity of insider and external C-A's against IO/ICS are given in the form of tuples:

$$RC = \langle EST, CE, SS_{ne}, SS_h, PP, O(NN) \rangle \ , \qquad (11)$$

$$IC_{l(m)} = \langle IST_l^{k-1}, CE, SS_{ne}, SS_h, PP, O^k(NN_m^k) \rangle , \qquad (12)$$

where *RC*– remote C-A against IO; $ICA_{l(m)}$ $IC_{l(m)}$ – internal C-A against IA with *k*-level of criticality, which are being processed in NN_m crosspoint, when an attacker has a user account with an access permission to a data, of which level of criticality is not higher than (*k*-1), and he is trying to increase his level of privileges; *EST* – external source of C-T; IST_l^{k-1} – insider source of C-T; *CE* – communication equipment in an information channel; SS_{ne}, SS_h – security services against the method of an C-A spreading (networked and host; *PP* – protocols and packets; *O* – access object; NN_m^k – IO/ICS crosspoint, on which information with the highest level of criticality (*k*) is processed; *l, m* – numbers of crosspoints.

The only effective way to identify an C-A is in the analysis of a combination of unusual events[16]. That is why in IDSS, an attack spreading *PSA* possible ways, quantity is compared to a quantity of indicators *DE*. The probability of the fact that suspicious action is a C-A is assessed with the indicators quantity which reacted against

the C-A spreading method[16],[17],[18]. Crossing $\tau_a(p_i)$ determines an indicators set. We get the following expression:

$$\zeta_a \subseteq PSA \cap DE = \\ = \{(psa_i, de_j) : psa_i \in PSA \cap de_j \in DE\}, \quad (13)$$

where DE = {de$_j$,..., de$_n$} – a network or IO perimeter indicator (detector); *PSA* – possible spreading ways of C-A's against IO/ICS crosspoints; $\zeta_a(psa_i)$ – crossing that determines an indicators set which reacts against the C-A on the recent method.

For solving a task in conditions of uncertainty, inconsistency and lack of knowledge about the information environment status under attack, mechanisms of fuzzy inference are activated in IDSS because of the fact that the MO system has some time limits for processing and analysing command information. Incoming information for a fuzzy inference module is the quantity and information value of unusual system events[19]. Information that is formed getting out of a fuzzy inference system corresponds to an outcome variable which is the probability of the fact that a group of unusual events in a network is an C-A[20].

There are some linguistic variables added to IDSS: «number of unusual events in network against the spreading of C-A», «number of unusual events in the host», «number of unusual events in IO perimeter», «probability of the fact that found unusual activity is an C-A». Following fuzzy sets A, B, C, D with membership functions $\upsilon_{\tilde{A}}, \upsilon_{\tilde{A}}, \upsilon_{\tilde{N}}, \upsilon_{\tilde{D}}$ are added to IDSS. Membership functions of linguistic variables for input and output variables and also for production memory are formed on the basis of expert estimate and results of modeling[21],[22].

In conditions when the status of the information environment is unknown, the C-T counteraction model is enabled in IDSS which has an opportunity to choose a controlling influence that better corresponds to the management object status.

---

[16] W. Kearney, H. Kruger, *Theorising on risk homeostasis in the context of information security behavior*, "Information and Computer Security" 2015, 24(5), pp. 496–513.

[17] O. Linda, M. Manic, T. Vollmer, J. Wright, *Fuzzy logic based anomaly detection for embedded network security cyber sensor*, "Computational Intelligence in Cyber Security (CICS), IEEE Symposium", 11–15 April 2011.

[18] L. Demetz, D. Bachlechner, *To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool*, "*The Economics of Information Security and Privacy*" 2013, Springer, Heidelberg.

[19] A. Oglaza, R. Laborde, P. Zarate, *Authorization Policies: Using Decision Support System for Context--Aware Protection of User's Private Data, Trust, Security and Privacy in Computing and Communications (TrustCom)*, "12th IEEE International Conference", July 2013.

[20] V. Lahno, *Ensuring of information processes' reliability and security in critical application data processing systems*, "MEST Journal", 2014, 2(1), pp. 71–79.

[21] M.M. Gamal, B. Hasan, A.F. Hegazy, *A Security Analysis Framework Powered by an Expert System*, "International Journal of Computer Science and Security (IJCSS)" 2011, 4(6).

[22] V. Lakhno, P. Kravchuk, D. Mekhed, H. Mohylnyi, V. Donchenko, *Development of a support system for managing the cyber protection of an information object*, "Journal of Theoretical and Applied Information Technology" 2017, 95(6), pp. 1263–1272.

A process of choosing an optimal safety events reaction variant are given in a form of a tuple:

$$\langle RO_i, RE_i, DA(RE_i), P_{CA}, P(z_l), OF, RO^r(\mathrm{P_{CA}})\rangle \quad 14$$

where RO_i – a reaction variant; RE_j – a result; DA_j – a damage assessment; z – environment status uncertainty characteristic; $P(z_l)$ – l environment status probability; OF – object function of choice; $RO^r(P_{CA})$ – rational variant of reaction; P_{CA} – C-A probability.

Safety events reaction variants probability analysis $\{\mathrm{RO_i}\}$ has shown that the number of control influences for each situation is limited $i \in [1,3]$.

An alternative advantages evaluation with a damage assessment model is used in IDSS – $\{RE_j\}, j \in [1,4]$ taking into account that the IS events reaction variants choice is made in conditions of a potential C-A: no harm, losses for a certain user, losses for a group of users, loss for all ICS from C-A realization[23],[24].

Define a function with which we choose an optimal reaction variant:

$$OF(RO_i, z) = \left(\sum_{l=1}^{s} DA_j\left(RE_j(RO_i, z_l)\right)\right) \cap \left(\prod_{i=1}^{I} p_j\left(RE_j(RO_i), P_{CA}\right)\right). \quad (15)$$

The probability p_{ij} of getting every j- result choosing every i- reaction variant is determined the following way:

$$\mathrm{p_{ij}} = \mathrm{p_{ij}}(\mathrm{RE_j}(\mathrm{RO_i}), \mathrm{P_{ca}}), \quad \forall i : \sum p_{ij} = 1 \ . \ (16)$$

Control influence rational variant $RO^r(P_{CA}^i)$ is determined this way:

$$\mathrm{RO^r}(\mathrm{P_{CA}}) = RO\left\{\arg\min_i\left(OF\left(RO_i, z\right)\right)\right\} \quad (17)$$

Threat counteraction methods are developed by an ISS analyst taking into account the possible cases of their spreading. They are developed on the basis of IDSS decision making method choice that is adapted to the reaction optimal variant choice: distant invasion through free-to-join networks, local network invasion, through a radio channel using a wireless hot spot or other[25,26,27].

---

[23] R.S. Gutzwiller, S.M. Hunt, D. S. Lange, *A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts, Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, "IEEE International Multi-Disciplinary Conference", 2016.

[24] L.P. Reesa, J.K. Deanea, T.R. Rakesa, W.H. Bakerb, *Decision support for Cybersecurity risk planning*, "Decision Support Systems" 2011, 51(3), pp. 493–505.

[25] S. Paliwal, R. Gupta, *Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm*, "International Journal of Computer Applications" 2012, 60(19), pp. 57–62.

[26] N. Ben–Asher, C. Gonzalez, *Effects of cyber security knowledge on attack detection*, "Computers in Human Behavior" 2015, 48, pp. 51–61.

[27] R. Verma, M. Kantarcioglu, D. Marchette, E. Leiss, T. Solorio, *Security Analytics: Essential Data Analytics Knowledge for Cybersecurity Professionals and Students*, "IEEE Security & Privacy" 2015, 13(6), pp. 60–65.

IP operational management intelligent support system is implemented in ISMS to negotiate difficulties with ill-defined situations and for increasing OM quality level[28].

An IS OM intelligent support subsystem contains: a fuzzy inference mechanism for C-A probability numeric evaluation; organized structure information about knowledge database (KD) events; C-T recognition and counteraction models[9,10,14]; algorithm for making a decision regarding choosing an optimal safety events reaction variant[13].

During the organizational-technical management process, the stage of planning of storage for information security tools, and the process of gradual removal of uncertainty about the structure and the storage of information security tools in the information security system is being considered[29],[30]. The process of planning *PL* rational sets *MIP* is described with the formula $PL = SFS \circledast CS_{al}$, where *SFS* – a range of functional sub-systems for perimeter IS; *CS* - chosen setup IST ($CS=\{CS_1,...CS_{AL}\}$), *AL* – the number of alternative setup variants, from which the choice is being made.

With the help of the system for intelligent support, the process of choosing optimal variant of *MIP* setup for perimeters of information security is considered as the formation of a sub-range for the best variants of setup $CS' \subseteq CS$.

By using the method of T. Saati[29] in the system of decisions support the evaluation of information security method and appropriate criteria is made. The normalized values of characteristic vectors of information security methods are calculated according to all criteria for "security" CR^1_{LS} and "expenses" CR^1_{in} indicators on the basis of the processing of all the matrices of pair-wise comparison taking into account the criteria connections.

3. Results of testing the software system «decision support system of management protection of ICS – DSSMPICS»

The software package "Decision Support System of Management protection of ICS – DSSMPICS» fig. 1, 2 designed for reasoned choice of a rational set of information security in the process of designing information security systems of information objects. DSSMPICS was also used in the modernization of existing information security systems in data centers of transport companies in Chernihiv (2016–2017), Dnipro (2014–2017), Poltava (2014–2015) and several industrial enterprises in Kyiv (Ukraine).

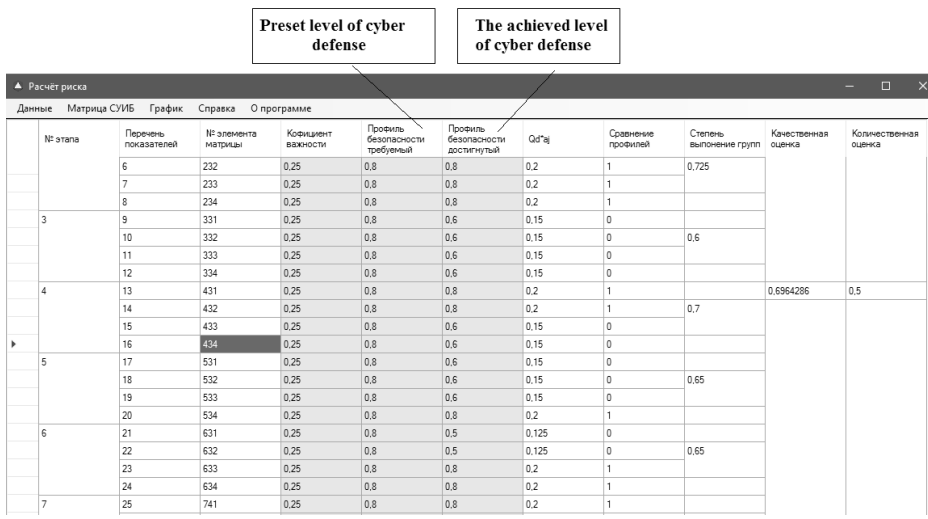
---

[28] J. Valenzuela, J. Wang, N. Bissinger, *Real-Time Intrusion Detection in Power System Operations*, "IEEE Transactions on Power Systems" 2013, 28(2), pp. 1052–1062.

[29] O.I. Garasymchuk, Y. M. Kostiv, *Assessment of the effectiveness systems protection of information* 2011, "Vestnik KNU imeni Mikhaila Ostrogradskogo", 1(66), pp. 12–34.

[30] V. Lakhno, Y. Tkach, T. Petrenko, S. Zaitsev, V. Bazylevych, *Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks*, "Eastern-European Journal of Enterprise Technologies" 2016, 9(84), pp. 32–44.

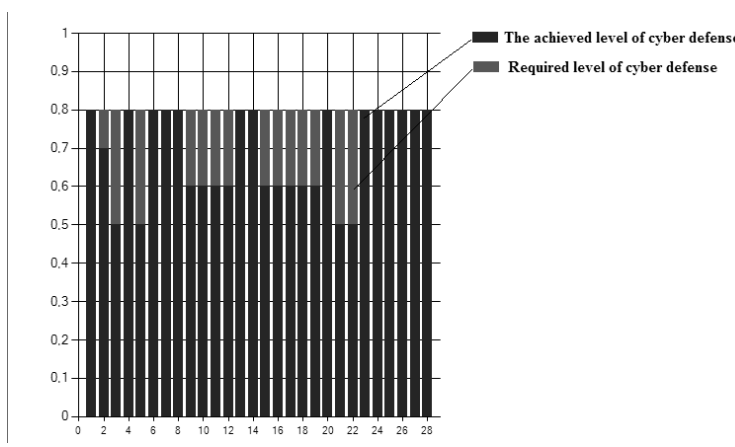
Figure 1. General view of the intelligent decision support of DSSMPICS
Rysunek 1. Ogólny widok inteligentnego wsparcia procesu decyzji DSSMPICS



№ этапа	Перечень показателей	№ элемента матрицы	Коффициент важности	Профиль безопасности требуемый	Профиль безопасности достигнутый	Qd*aj	Сравнение профилей	Степень выпонение групп	Качественная оценка	Количественная оценка
	6	232	0,25	0,8	0,8	0,2	1	0,725		
	7	233	0,25	0,8	0,8	0,2	1			
	8	234	0,25	0,8	0,8	0,2	1			
3	9	331	0,25	0,8	0,6	0,15	0			
	10	332	0,25	0,8	0,6	0,15	0	0,6		
	11	333	0,25	0,8	0,6	0,15	0			
	12	334	0,25	0,8	0,6	0,15	0			
4	13	431	0,25	0,8	0,8	0,2	1		0,6964286	0,5
	14	432	0,25	0,8	0,8	0,2	1	0,7		
	15	433	0,25	0,8	0,6	0,15	0			
	16	434	0,25	0,8	0,6	0,15	0			
5	17	531	0,25	0,8	0,6	0,15	0			
	18	532	0,25	0,8	0,6	0,15	0	0,65		
	19	533	0,25	0,8	0,6	0,15	0			
	20	534	0,25	0,8	0,8	0,2	1			
6	21	631	0,25	0,8	0,5	0,125	0			
	22	632	0,25	0,8	0,5	0,125	0	0,65		
	23	633	0,25	0,8	0,8	0,2	1			
	24	634	0,25	0,8	0,8	0,2	1			
7	25	741	0,25	0,8	0,8	0,2	1			

Source: Authors´ own research (2017).

Figure 2. Simulation results module with used DSSMPICS
Rysunek 2. Moduł wyników symulacji z użyciem DSSMPICS



Source: Authors´ own research (2017).

On the software «DSSMPICS», that particular selection method implemented an efficient option for responding to security events. The results are shown in Table 1.

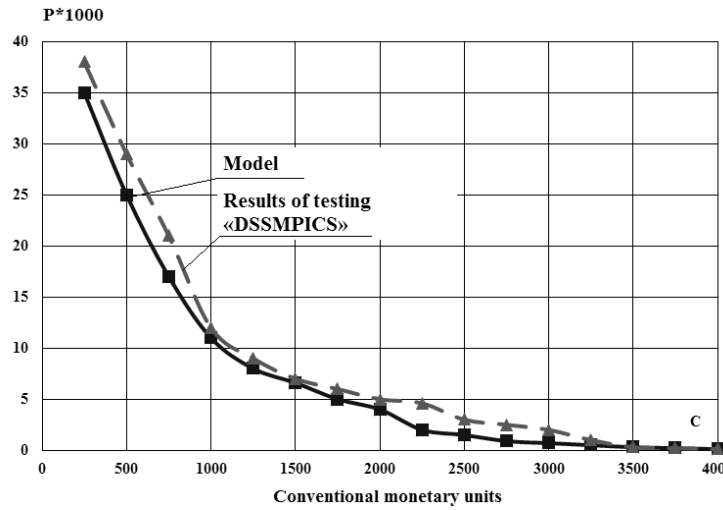
Table 1. The results of testing the software system DSSMPICS»
Tabela 1. Wyniki testowania oprogramowania systemu DSSMPICS

Class of C-A	**Options for responding to the current settings information of environment of IO/ICS**		
U2R	A=2, B=3, P_a = 0,54		A=1, B=1, P_a = 0,242
	A=1, B=2, P_a = 0,48		A=2, B=1, P_a = 0,21
	The end of session attack source node		Sending a warning message to the user (Sending m-u)
R2L	A=1, B=3, P_a = 0,43		A=1, B=1, P_a = 0,192
	A=1, B=2, P_a = 0,38		A=2, B=2, P_a = 0,27
	The end of session attack source node		(Sending m-u)
DOS/ DDOS	A=2, B=3, P_a = 0,62 and A=1, B=2-3, P_a = 0,5-0,65		A=1, C=2, P_a = 0,4 and A=1, C=1–2, P_a =0,3–0,4
	A=1, B=2, P_a = 0,62 and A=2, B=3, P_a = 0,65-0,69		A=1, C=2, P_a = 0,4 and A=2, C=2-3, P_a =0,36–0,47
	The end of session attack source node		(Sending m-u)
The external C-A via Wi Fi	A=3, C=3, P_a = 0,678	A=1, C=2, P_a = 0,4	A=1, C=1, P_a = 0,3
	A=2, C=3, P_a = 0,62	A=2, C=2, P_a = 0,4	A=1, C=3, P_a = 0,36
	Blocking access point	DOS-attack on stations	The lack of response
Network Scanning	A=2, B=3, P_a = 0,45 and A=1, B=2-3, P_a = 0,4-0,51	A=1, C=2, P_a = 0,37 and A=1, C=1–2, P_a =0,32–0,46	A=1, C=2, P_a = 0,36 and A=1, C=1–2, P_a =0,33–0,45
	The end of session attack source node		
Cross Site Scripting	A=1–3, C=1–2, P_a = 0,45–0,65	A=2, C=1, P_a = 0,42	A=1, C=2, P_a = 0,27
	The end of session attack source node		

Source: Authors´ own research (2017).

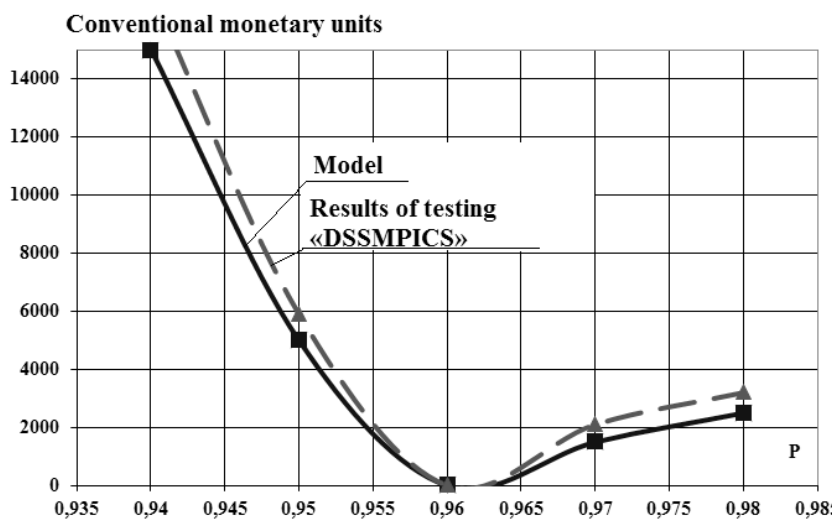
Figures 3, 4 show examples of simulation results by using DSSMPICS rational sets of information security.

Figure 3. The dependence of the probability of an attacker on the cost of CS of an IO/ ICS
Rysunek 3. Zależność prawdopodobieństwa ataku od kosztu CS dla IO / ICS



Source: Authors´ own research (2017).

Figure 4. The integral indicator of overall spending on CS and the probability of successful offensive counter data protection
Rysunek 4. Integralny wskaźnik całkowitych wydatków na rzecz CS oraz skuteczna ofensywna ochrona przeciwkradzieżowa danych



Source: Authors´ own research (2017).

On Fig. 3 are common simulation results, which show that with the increase in the provision for information security of information objects, the probability of attackers' success of all goals is greatly reduced. Fig. 4 the dependence of the integral index of overall spending on information security system for the information object related to losses from the actions of the offender and the cost of organizing rational alternative sets of information security. The dependence has a pronounced minimum. This indicates that from this point of spending on information security, the information object system begins to exceed the losses from the actions of the offender, and therefore the bulk of the integral index is the total cost of information security.

During the research the possibility was taken into account of an C-A that implements remote intrusion through the perimeter, the availability of internal and external users, and abusers that have high privileges and violate the safety of information. After the formation of efficient information security in enterprises which took part in the study, with the help of intelligent decision support «DSSMPICS» the predicted value was 1,8–1,9% risk that there was an average value of 5,85–6,17 times less risk to information security systems compared to before.

The approach of building a comprehensive information security system for the information object makes it possible to reduce the cost of data protection by 31–34% compared to alternative methods[11, 12, 14, 17, 18, 22].

Further development of this work may be improving the interaction of traditional mechanisms of information security of IO/ICS, which, in particular, are working on primary information system modules and intelligent decision support «DSSMPICS».

Overall, based on the studies, we can ascertain the effectiveness of the proposed models and software for information security management (information systems and automated control system) in examined enterprises.

Conclusions

1. The model of operational management information and CS object forms a rational set of remedies based on morphological approach. Unlike existing solutions, the model prepared on the basis of intelligent decision support, a morphological matrix for each facility's perimeters of information protection, and can generate a set of options for remedies which take into account the compatibility of software and hardware. The choice of the optimal option set for that perimeter protection of information, implements an objective function that maximizes the ratio of the sum "security information" to the total rate "cost." It provides a range of remedies for a given class of certified security, and satisfies the requirements for eligible costs for implementation of information security.

2. A developed software suite was made for intelligent decision support circuits organizational, technical and operational management of information system protection facilities. It confirmed the adequacy of the proposed models and algorithms. By using the developed system of intelligent decision support, networks of enterprises using DSSMPICS reduced the projected cost of the planned system of protection to 34%.

References

Al-Jarrah O., Arafat A., *Network Intrusion Detection System using attack behavior classification*, "Information and Communication Systems (ICICS)", 5th International Conference, 2014.

Atymtayeva L., Kozhakhmet K., Bortsova G., *Building a Knowledge Base for Expert System in Information Security*, Chapter Soft Computing in Artificial Intelligence of the series Advances in "Intelligent Systems and Computing", Vol. 270, 2014.

Ben–Asher N., Gonzalez C., *Effects of cyber security knowledge on attack detection*, Computers in Human Behavior, 48, 2015.

Bosak I.P., Palyha Ie.M., *Informatsiine zabezpechennia upravlinnia pidpryiemstvom: ekonomichnyi aspect,* "Rehionalna ekonomika", 4, 2007.

Cavusoglu H., Srinivasan R., Wei T.Y., *Decision-theoretic and game-theoretic approaches to IT security investment*, "Journal of Management Information Systems (ACySe)", 25(2), 2008.

Demetz L., Bachlechner D., *To Invest or Not to Invest? Assessing the Economic Viability of a Policy and Security Configuration Management Tool*, "The Economics of Information Security and Privacy", Springer, Heidelberg, 2013.

Gamal M.M., Hasan B., Hegazy A.F., *A Security Analysis Framework Powered by an Expert System*, "International Journal of Computer Science and Security", 4(6), 2011.

Garasymchuk O.I., Kostiv Y.M., *Assessment of the effectiveness systems protection of information*, "Vestnik KNU imeni Mikhaila Ostrogradskogo", 1(66), 2011.

Gutzwiller R.S., Hunt S.M., Lange D.S., *A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts*, Cognitive Methods in Situation Awareness and Decision Support (CogSIMA), "IEEE International Multi-Disciplinary Conference", 2016.

Kaliuzhnyi R., Shvets M., Shamrai V. [in:] Kaliuzhnoho R., Shamraia V. *Informatsiine zabezpechennia upravlinskoi diialnosti v umovakh informatyzatsii: orhanizatsiino-pravovi pytannia teorii i praktyky,* Kiyv, 2002.

Kanatov M., Atymtayeva L., Yagaliyeva B., *Expert systems for information security management and audit*, Implementation phase issues, Soft Computing and Intelligent Systems (SCIS), Joint 7th "International Conference on and Advanced Intelligent Systems (ISIS)", 2014.

Kearney W., Kruger H., *Theorising on risk homeostasis in the context of information security behavior*, "Information and Computer Security", 24(5), 2015.

Koposov H.A., Nahornaia Y.Y., *Pryntsypy ekonomycheskoi bezopasnosty predpryiatyia,* II Mizhnarodnoi naukovoi konferentsii, Cherkasy 2005.

Lakhno V., Malyukov V., Domrachev V., Stepanenko O., Kramarov O., *Development of a system for the detection of cyber attacks based on the clustering and formation of reference deviations of attributes*, „Eastern-European Journal of Enterprise Technologies" 2017, 3/9 (87).

Lahno V., *Ensuring of information processes' reliability and security in critical application data processing systems*, "MEST Journal", 2(1), 2014.
Lakhno V., Petrov A., *Ensuring security of automated information systems, transportation companies with the intensification of traffic*, Ukraine, 2011.
Lakhno V., Tkach Y., Petrenko T., Zaitsev S., Bazylevych V., *Development of adaptive expert system of information security using a procedure of clustering the attributes of anomalies and cyber attacks*, "Eastern-European Journal of Enterprise Technologies", 9(84), 2016.
Lakhno V.A., Kravchuk P.U., Mekhed D.B., Mohylnyi H.A., Donchenko V.U., *Development of a support system for managing the cyber protection of an information object*, "Journal of Theoretical and Applied Information Technology", 95(6), 2017.
Linda O., Manic M., Vollmer T., Wright J., *Fuzzy logic based anomaly detection for embedded network security cyber sensor*, "Computational Intelligence in Cyber Security (CICS)", IEEE Symposium on 11–15 April 2011.
Li-Yun Chang, Zne-Jung Lee, *Applying fuzzy expert system to information security risk Assessment – A case study on an attendance system*, "International Conference on Fuzzy Theory and Its Applications" 2013.
Louvieris P., Clewley N., Liu X., *Effects-based feature identification for network intrusion detection*, Neurocomputing, 121(9), 2013.
Oglaza A., Laborde R., Zarate P., *Authorization Policies: Using Decision Support System for Context-Aware Protection of User's Private Data, Trust,* "Security and Privacy in Computing and Communications (TrustCom)", 12th IEEE International Conference on 16–18 July 2013.
Paliwal S., *Gupta R. Denial-of-Service, Probing & Remote to User (R2L) Attack Detection using Genetic Algorithm*, "International Journal of Computer Applications", 60(19), 2012.
Panaousis E., Fielder A., Malacaria P., Hankin C., Smeraldi F., *Cybersecurity Games and Investments: A Decision Support Approach*, Chapter "Decision and Game Theory for Security" of the series Lecture Notes in Computer Science, 8840, 2014.
Reesa L.P., Deanea J.K., Rakesa T.R., Bakerb W.H., *Decision support for Cybersecurity risk planning*, "Decision Support Systems", 51(3), 2011.
Tkachuk T.P., *Formuvannia systemy informatsiinoi bezpeky biznesu,* "Biznes i bezpeka", 4, 2009.
Tsymbaliuk V.S. *Informatsiina bezpeka pidpryiemnytskoi diialnosti: vyznachennia sutnosti ta zmistu poniattia za umov vkhodzhennia Ukrainy do informatsiinoho suspilstva (hlobalni kibertsyvilizatsii),* "Pidpryiemnytstvo, hospodarstvo i parvo", 3, 2007.
Valenzuela J., Wang J., Bissinger N., *Real-Time Intrusion Detection in Power System Operations*, "IEEE Transactions on Power Systems", 28(2), 2013.
Verma R., Kantarcioglu M., Marchette D., Leiss E., Solorio T., *Security Analytics: Essential Data Analytics Knowledge for Cybersecurity Professionals and Students*, "IEEE Security & Privacy", 13(6), 2015.
Zhang Y., Wang L., Sun W., Green R.C., Alam M., *Distributed Intrusion Detection System in a Multi-Layer Network Architecture of Smart Grids*, "IEEE Transactions on Smart Grid", 2(4), 2011.

Author`s resume:
Professor Dr Valeriy Lakhno,
Department of Managing Information Security, European University.

Professor Dr. hab. Eng. Alexander Petrov,
AGH University of Science and Technology Faculty of Management.

PhD Inna Nagorna,
PhD, Dean of the Faculty of Enterprise Security, European University.

Nota o Autorach:
Prof. Dr Valeriy, Lakhno
Departament Zarządzania Bezpieczeństwem Informacji, Uniwersytet Europejski.

Prof. Dr hab inż. Alexander Petrov,
AGH, Kraków, Wydział Zarządzania, Katedra Informatyki Stosowanej

PhD Inna Nagorna,
PhD, Dziekan Wydziału Bezpieczeństwa Przedsiębiorczości, Uniwersytet Europejski.

Contact/Kontakt:
Valeriy Lakhno
Department of Managing Information Security, European University
16B Academician Vernadskiy blvd., Kyiv, Ukraine, 03115
E-mail: valss21@ukr.net

Alexander Petrov
AGH University of Science and Technology Faculty of Management, Gramatyka 10, 30-067 Krakow, phone: +48 886818122
E-mail: asp1951@gmail.com

Inna Nagorna
Dean of the Faculty of Enterprise Security, European University.
16B Academician Vernadskiy blvd., Kyiv, Ukraine, 03115
E-mail: Inna_nagornay@mail.ru

The contribution of particular co-authors to preparation of the paper:
Wkład poszczególnych autorów w przygotowanie publikacji:
Valeriy Lakhno – 33,34%, Alexander Stepanovich – 33,33%, Inna Nagorna – 33,33%.