UDC 004.056:336.71 DOI: 10.30748/nitps.2019.37.15

O. Milov, S. Milevskyi, O. Korol

S. Kuznets Kharkiv National University of Economics, Kharkiv

DEVELOPING AN ADVANCED CLASSIFIER OF THREAT FOR SECURITY AGENT BEHAVIOR MODELS

The modern development of high technologies and computer technology has had a significant impact on the development of business process management systems, covering all areas of the state economic activity. However, in parallel with this, the era of high technologies has significantly expanded the range of threats aimed at the contour of business processes, and, first of all, on information resources that ensure the functioning of the business process circuit. At the same time, threats have acquired signs of hybridity and synergy. In these conditions, the urgent issue in the formation of the information security management system of the business process circuit is the timely detection and subsequent analysis of modern threats. In order to generalize the approach of classifying hybrid cyber threats into security components: information security (IS), cybersecurity (CS), security of information (SI) of the business process circuit and their information resources, an advanced classifier of threats to the business process circuit and its information resources is proposed, including cost estimates of the threats implementation and estimates of losses associated with threats. The proposed extensions to the threat classifier allow to give probabilistic assessments of the implementation of certain threats. Based on the analysis of approaches, estimates of indicators of the intruders danger degree and the degree of protective measures implementation under the conditions of modern hybrid cyber threats are proposed.

Keywords: *informational resources; Information Security; hybrid cyberthreats; contour of business processes; threat classifier.*

Introduction

In modern conditions of mass accessibility of computer systems and telecommunications, increasing the turnover of electronic document management, and the transition to electronic commerce, the problems of cybersecurity at all levels of government are greatly exacerbated. As a result, losses from security breaches are becoming increasingly expensive for various companies, the state as a whole, and for individual citizens [1].

The analysis of international standards and standards of Ukraine [2] showed that the individual components of the methodology for assessing the security of information technologies based on a security model – ensuring integrity, confidentiality and accessibility (ICA models) were considered. At the same time, there is no synergistic approach to the analysis of cyber threats, a unified methodology for assessing the security of information technologies in various sectors of the economy, which does not allow for the timely formation of relevant policies, new approaches and measures to ensure cyber security of the business processes of organizations.

Formulation of the problem. An integral part of building the security system business process circuit is the formation of a management system based on the classification of all components of a security system. An integral part of the problem of ensuring cybersecurity is the task of risk analysis. In fact, risk is an integral assessment of how effectively existing defenses are able to withstand attacks on the organization's business processes. Despite the fact that many mechanisms and means of information protection have been developed, today one of the priority tasks remains the task of assessing the effectiveness of the process of ensuring the safety of the business process circuit based on relevant metrics. As analysis [3–11] showed, among the most common safety metrics are their taxonomies such as: Vaughn-Hennig-Siraj, NIST STS822, OCIPEP, OCTAVE, CISWG, Erkan Kahraman. Recently, most researchers are inclined to the idea that the social and behavioral characteristics of security processes play a major role [13–14]. Therefore, the existing and used threat classification schemes that underlie the processes for ensuring the security of the business process circuit must be substantially changed by adding cost indicators of the threat realization that determine the motivation for the behavior of attackers. Added indicators together with assessments of implementation risks will make it possible to formulate assessments which of the threats are most preferable and which resources should be directed first to protection.

The aim of the article. The aim of the article is to build an improved threat classifier based on a synergistic approach and assessing indicators of the attackers-danger degree and the degree of protective measures implementation, taking into account both the motivational elements of attackers, expressed in the probabilistic characteristics of the implementation of threats, and

cost indicators of assessing the damage caused by the implementation of the respective threats.

Research results

The main object of cyberattacks should be considered the outline of the organization's business processes. An organization's business process (BP)contour is a set of business processes and their implementation of information resources, the implementation of which in a given sequence leads to the achievement of the organization's goals, which can be described as follows:

$$S^{BP} = \left\{ \left\langle S^{BP1}, IR^{BP1}, T^{BP1} \right\rangle, ..., \left\langle S^{BP_n}, IR^{BP_n}, T^{BP_n} \right\rangle \right\},$$

where S^{BP} – the contour of business processes as a set of BP, each of which represents:

S^{Bpi} – *i*-th business process, defined by the relationship structure of individual business operations performed in a specific sequence;

IR^{BPi} – set of information resources of the *i*-th business process;

T^{BPi} – set of threats to the *i*-th business process.

Ensuring the protection of the organization's business processes can be represented similar to the BP contour, but the security system. The security system business process circuit is a set of business processes and the resources necessary for them, the implementation of which ensures the normal functioning of the organization's business process circuit. This BP loop can be represented similarly, namely:

$$S^{BS} = \left\{ \left\langle S^{BS_1}, Rs^{BS_1}, T^{BS_1} \right\rangle, ..., \left\langle S^{BS_m}, Rs^{BS_m}, T^{BS_m} \right\rangle \right\},$$

where S^{BP} – the contour of business processes of the security system as a set of BP, each of which represents:

S^{BSi} – *i*-th business process defined by the structure of the links of individual business operations performed in a specific sequence in the security system;

IR^{BSi} – set of information resources protected by the *i*-th business process of the security system;

T^{BSi} – a set of threats that the *i*-th business process of the security system provides protection against.

The interaction of the presented circuits in the process of functioning is shown in Fig. 1.

The basis of the functioning of the BP contour of a security system is the set of threats presented in the classifier, for the description of which appropriate metrics must be defined. To construct threat metrics based on the synergistic approach proposed in [15], we will use the approach to construct a threat classifier based on the information-analytical model of the double triples method proposed in [16–20]. In contrast to the classifier known in the construction of the classifier, the substantive part of each of the four platforms includes a number of components, respectively.

The first platform is the classification of threats according to the security components of the business process information resources: information security (IS) (01), security of information (SI) (02), cybersecurity (CS) (03). We introduce the following definitions.

Definition 1. Security of the business process contour – the state of security of business processes and their information resources, characterized by the ability of performers, technical means and information technologies to ensure the confidentiality, integrity, authenticity and availability of resources required for the implementation of business processes in the circuit of the corresponding level.

Definition 2. Resource security of the business process contour (RSBPC) is the state of security of the KBP resource environment, which ensures its formation, use and development in the interests of business process owners.

Definition 3.Cybersecurity of the business process circuit – a set of tools, strategies, security principles, security guarantees, risk management approaches, actions, training, insurance and technologies that are used to protect the cyber environment of the business process contour, resources and users of business processes.

The second platform is the classification of threats according to the nature of their orientation: regulatory (01), organizational (02), engineering (03).

The third platform is the classification of threats in accordance with the main features of information: confidentiality (01), integrity (02), accessibility (03), authenticity (04).

The fourth platform is a classification of threats according to the hierarchy levels of the business process circuit infrastructure: PL – physical layer (01), NL – network layer (02), OSL – layer of operating systems (OS) (03), DBL – layer of database management systems (04), BL – layer of technological applications and services (05).

The use of the proposed classifier is implemented as a sequence of the following steps.

Step 1. Formation of metric coefficients for risk factors by security services experts. Let j will be security services for the resources of business processes. The main security services are C – confidentiality, I – integrity, A – availability, Au – authenticity. Then the classifier for the four security services is described by an expression of the form $j = \{C, I, A, Au\}$.

Lets evaluate the weighting coefficients of the manifestation of each of the *N* threats presented in the classifier. *K* experts participate in determining the weighting factors for the manifestation of each threat to resource security services. In addition, to determine the potential damage, each threat is classified according to the criterion of criticality of causing damage to the business processes of the organization as a whole.

According to the ISO / IEC15408 standard, experts choose a quality level of damage: critical, high, medium, low. Using risk assessment techniques CRAMM or FAIR, you can evaluate the qualitative level in quantitative terms.

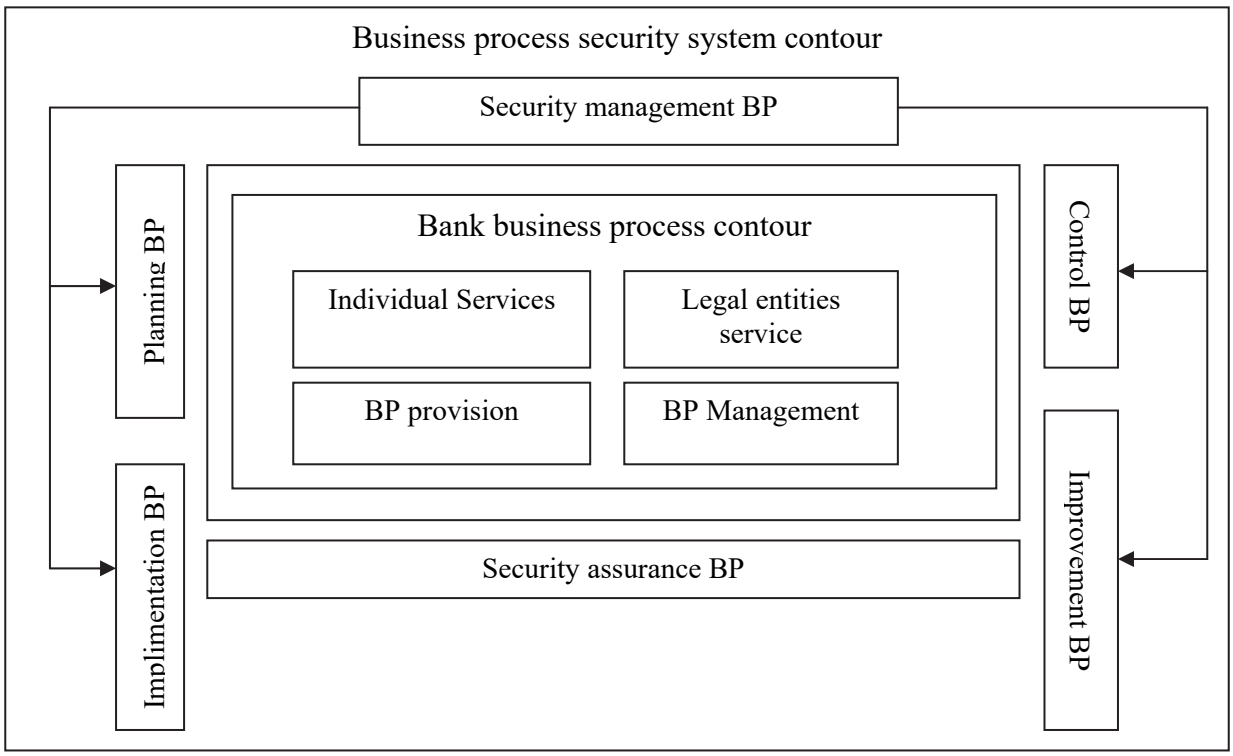

Fig. 1. The interaction of the business processes and the security system

Thus, at the first step, weights are generated for the metrics of modern hybrid cyberthreats, which allows them to be used within the SIEM system (Security Information and Event Management) in order to simplify the audit and correlation of information from various sources.

Lets denote by i the current threat number $\left(\{i\}_1^N\right)$, k – current expert number, which evaluated $\left(\{k\}_1^K\right)$.

The average expert rating of all threats for a particular security service can be recorded as:

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j ,$$

where w_{ik}^j – value of the metric coefficient set by the k-th expert for the i-th threat of the j-th security service; N – number of threats; K – number of experts.

Step 2. he formation of threat identifiers by the components of the classifier. At this stage, the experts form the digital value (code) of the threat identifier according to the corresponding components of the classifier.

Step 3. The choice of weight coefficients a_i, that determine the conditions for the manifestation of the i-th threat (Tabl. 1) [21–22].

Step 4. Determining the implementation of each i-th threat, taking into account the probability of an attack (its occurrence) is carried out according to:

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j .$$

Table 1

Table for selecting weighting coefficients a_i manifestations of a threat depending on the conditions for its manifestation

Weighting coefficients a_i	Threat Conditions
0,067	the threat occurs not more than once every 5 years
0,133	the threat does not occur more than once a year
0,2	the threat does not occur more than once a month
0,267	the threat does not occur more than once a week
0,333	the threat occurs every day

For each security service and i-th threat:

$$w_i^C \alpha_i^C = \frac{1}{K}\alpha_i^C \sum_{k=1}^{K} w_{ik}^C \quad \text{service "confidentiality"}$$

$$w_i^I \alpha_i^I = \frac{1}{K}\alpha_i^I \sum_{k=1}^{K} w_{ik}^I \quad \text{service "integrity"}$$

$$w_i^A \alpha_i^A = \frac{1}{K}\alpha_i^A \sum_{k=1}^{K} w_{ik}^A \quad \text{service "availability"}$$

$$w_i^{Au} \alpha_i^{Au} = \frac{1}{K}\alpha_i^{Au} \sum_{k=1}^{K} w_{ik}^{Au} \quad \text{service "authenticity",}$$

where $w_{ik}^{C}, w_{ik}^{I}, w_{ik}^{A}, w_{ik}^{Au}$ – expert security service weights: confidentiality, integrity, accessibility, authenticity;

$\alpha_i^C, \alpha_i^I, \alpha_i^A, \alpha_i^{Au}$ – security service weights: confidentiality, integrity, accessibility, authenticity of attack manifestation and i-th threat.

Step 5. Determining the implementation of the occurrence of several threats for the selected service is calculated as follows:

$$W_{syn}^{C} = \sum_{i=1}^{M} w_i^C \alpha_i^C \quad \text{service “confidentiality”}$$

$$W_{syn}^{I} = \sum_{i=1}^{M} w_i^I \alpha_i^I \quad \text{service “integrity”}$$

$$W_{syn}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A \quad \text{service “availability”}$$

$$W_{syn}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \quad \text{service “authenticity”},$$

where M – the number of several threats that are selected by the information security expert from the set $\{i\}_i^M$, which is a subset of the entire set of classifier threats, i.e. $M \le N$. When determining the implementation of the occurrence of several threats for the selected service, the indicator with the highest value among all is selected.

When forming metric coefficients, it is believed that the results obtained are related to independent threats, in case of their dependence, it is necessary to use the expression for determining the total probability of dependent events:

$$P(AB) = P(A) + P(B) - P(AB).$$

Statistical processing of the results of the assessment of the possibility of the influence of the *i*-th threat on the security service by experts is carried out according to the method described in [23]. The final assessment of the *i*-th threat is averaged over the number of experts in accordance with the expression:

$$x_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K},$$

where x_k- assessment of the impact of the *i*-th threat given by the *k*-th expert;

k_k – competency level of the *k*-th expert;

K – number of experts.

A measure of the consistency of expert opinions is considered to be the variance calculated in accordance with the expression:

$$\sigma_x^2 = \frac{1}{K} \sum_{k=1}^{K} k_k (x_k - x_i)^2.$$

The statistical significance of the results with probability $1 - \alpha_i$, makes up:

$$[x_i - \Delta, x_i + \Delta],$$

where the value x_i distributed according to normal law centered at x_i and dispersion σ_x^2. Then Δ defined as the value of an expression:

$$\Delta = t\sqrt{\sigma_x^2 / N},$$

where t – value obeying student distribution for K–1 degrees of freedom; K – number of experts.

Step. 6. The definition of the total threat by security components, taking into account expression (3), is calculated:

$$W_{syn}^{IB} = \sum_{i=1}^{N} (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) \alpha_i;$$

$$W_{syn}^{KB} = \sum_{i=1}^{N} (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) \alpha_i;$$

$$W_{syn}^{BI} = \sum_{i=1}^{N} (w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au}) \alpha_i.$$

When determining the implementation of the occurrence of several threats for the selected service, an indicator α_i is selected with the highest value among all.

Step 7. Determination of the generalized synergetic threat to the business process circuit:

$$W_{syn}^{IB,KB,BI} = W_{syn}^{IB} \cup W_{syn}^{KB} \cup W_{syn}^{BI}.$$

Step 8. The definition of a generalized synergistic threat, taking into account its hybridity, is calculated as follows:

$$W_{syn}^{hibrid\,C,I,A,Au} = W_{syn}^{C} \cap W_{syn}^{I} \cap W_{syn}^{A} \cap W_{syn}^{Au}.$$

It is proposed to introduce a new platform into the threat classifier – the platform of attack cost indicators. This will allow to evaluate threats from the point of view of economic efficiency of their use and counteraction to them.

Improving the classifier of threats through the introduction of cost indicators of threats allows implementing an algorithm for constructing a rating of potential threats and the importance of information resources to be protected, is presented in Fig. 2.

The proposed algorithm implements the following actions. Both sides of the attack are determined by the importance (rating) of the attacks that are economically feasible.

1st step. Those attacks are determined whose effect of the implementation exceeds the costs of their implementation.

$$Tr_R^A = \left\{ Tr_i \mid \left(P_i^A - C_i^A \right) > 0 \right\} \forall Tr_i \in Tr,$$

where Tr_R^A – many potential threats that are effective for the attacker;

Tr_i – threat to the *i*-th information resource;

P_i^A – assessment of the cost of success of the attack on the *i*-th resource of the business process by the attacker;

C_i^A – the cost of an attack on the *i*-th resource of a business process by an attacker.

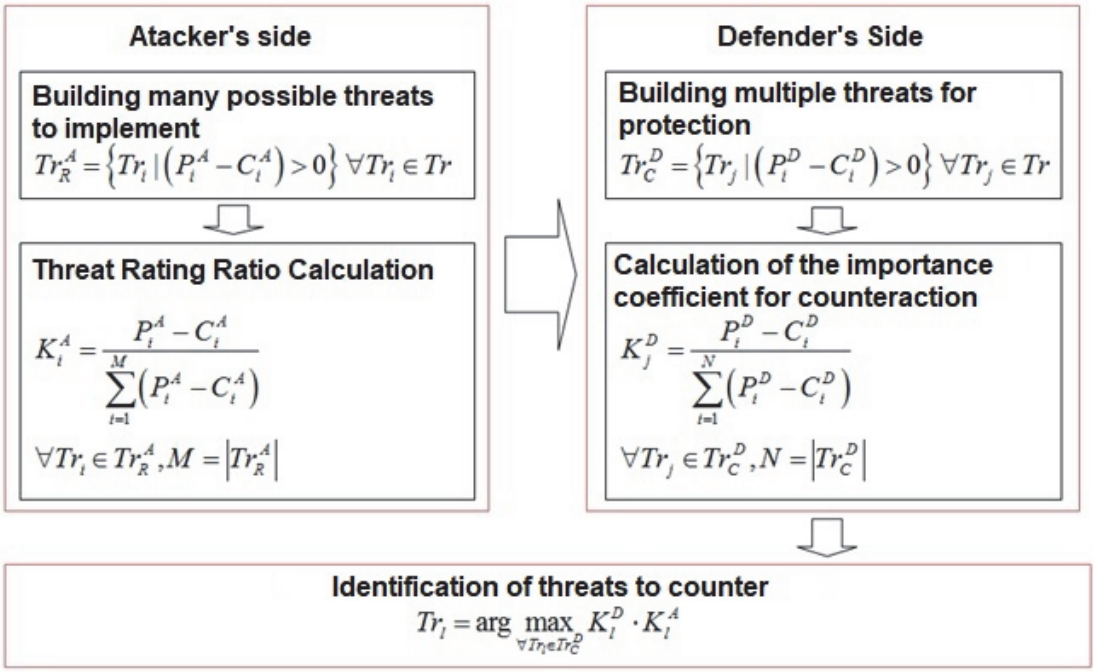

Fig. 2. Determining the most probable threat to implementation

2nd step. Similarly, the directions of protection are determined that provide an effect higher than the costs of their provision.

$$Tr_C^D = \left\{Tr_j \mid \left(P_i^D - C_i^D\right) > 0\right\} \forall Tr_j \in Tr,$$

where Tr_C^D – many threats against which it is economically feasible to build protection;

P_i^D – estimation of the cost of the loss of the *i*-th information resource for the defense side;

C_i^D – the cost of protecting the *i*-th information resource for the protection side;

3rd step. The importance factors for attackers are defined as the share of the winnings of the total winnings, which can be obtained potentially when implementing the whole complex of threats for attackers:

$$K_i^A = \frac{P_i^A - C_i^A}{\sum_{i=1}^{M}\left(P_i^A - C_i^A\right)}$$

$$\forall Tr_i \in Tr_R^A, M = \left|Tr_R^A\right|,$$

where K_i^A – rating coefficient (importance) of threat realization to the i-th information resource;

M – the power of a multitude of selected potentially effective threats to the attacker.

4th step. The importance factors for defenders are defined as the share of the winnings of the total winnings that can be obtained potentially when implementing the entire range of protective measures:

$$K_j^D = \frac{P_i^D - C_i^D}{\sum_{i=1}^{N}\left(P_i^D - C_i^D\right)},$$

$$\forall Tr_j \in Tr_C^D, N = \left|Tr_C^D\right|$$

where K_j^D – rating coefficient (importance) of building the protection of the *j*-th information resource.

5th step. As the most probable threat that can be realized, one of them is selected for which the product of the importance coefficients of the attacker and the attacker is the maximum:

$$Tr_l = \arg \max_{\forall Tr_\eta \in Tr_C^D} K_l^D \cdot K_l^A.$$

Conclusions

The proposed model allows to determine the most likely threats aimed at violating the security of information resources and, as a result, economically justify the distribution of limited funds between various information resources requiring protection. In the absence of statistics, cost estimates of threats can be obtained by expert methods, as described above.

The model for determining the most probable threat makes it possible to organize the effective distribution of limited funds to protect the resources of the business process circuit based on the use of the results

of modeling the behavior of cooperative antagonistic agents to determine and calculate the probability of a threat. It should be noted that the proposed additions to the classification of threats are a reflection of the behavior of all parties to the conflict under the conditions of synergy and hybridity of threats and can explain the motivation of behavior of all parties to the conflict.

References

1.Grischuk, R.V. and Danik, Yu.G. (2016), "*Osnovy kiberbezpeky*" [*Basics of Cybersecurity*], ZhNAEU, Zhytomyr, 636 p.

2. Evseev, S.P. (2018), "Klasyfikator kiberzahroz informatsiinykh resursiv avtomatyzovanykh bankivskykh system" [Cyber Threat Classifier for automated service systems information resources], *Cybersecurity: education, science, technology*, No. 2(2), pp. 47-67.

3. U.S. Department of Defense (1985), *Trusted Computer Systems Evaluation criteria*, US DoD 5200.28-STD, available at: https://csTe.mst.gov/csTe/media/pubtications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf (accessed 7 December 2017).

4. Office for Official publications of the European Communities (1991), *Information Technology Security Evaluation Criteria v. 1.2.*, available at: https://www.bsi.bund.de/SharodDocs/Dowrdoads/DE/BSrZertifizierung/ITSicherheitskriterien/itsec-enjxff.pdf?_blob=pubticationFile (accessed 7 December 2017).

5. Canadian System Security Centre, Communications Security Establishment (1993), *Canadian Trusted Computer Product Evaluation Criteria v. 3.0*, Government of Canada, available at: www.btb.tenniurnplus.gc.ca/tpv2alpha/alpha-eng.lrtml?lang=eng&i=&index=alt&srclrtxt=CANADIAN%20TRUSTED%20COMPUTER%20PRODUCT%20EV ALUATION%20CR1TERIA (accessed 7 December 2017).

6. NIST, NSA, US Government (1993), *Federal Criteria for Information Technology security*, available at: https://www.cotmnoncriteriaportal.org/files/ccfiles/ccpartlv2.3.pdf (accessed 7 December 2017).

7. ISO/1EC 15408-1:1999 (1999), *Information technology – Security techniques – Evaluation criteria for IT security – Part I: Introduction and general model*, available at: https://www.iso.org/ni/standard/27632.html (accessed 7 December 2017).

8. ISO/1EC 15408-2:2005 (2005), *Information technology – Security techniques – Evaluation criteria for ГТ security – Part 2: Security functional requirements*, available at: https://www.iso.org/ru/standard/40613.html (accessed 7 December 2017).

9. ISO/IEC 15408-3:2008 (2008), *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements*, available at: https://www.iso.org/ru/standard/46413.html (accessed 7 December 2017).

10. CEM-97A)17. *Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model*.

11. Horbenko, Y.D., Potii, A.V. and Tereshchenko, P.Y. "*Kryteryy y metodolohyy otsenky bezopasnosty ynformatsyonnykh tekhnolohyi*" [*Criteria and methodologies for assessing the security of information technology*], available at: www.bezpeka.com/ni/hb/spec/infsys/artl08.html.

12. Evseev, S. (2017), "Model narushytelia prav dostupa v avtomatyzyrovannoi bankovskoi systeme na osnove synerhetycheskoho podkhoda" [A model of access rights violator in an automated banking system based on a synergistic approach], *Informational security*, No. 2(26), pp. 110-120.

13. Mylov, A.V. and Korol, O.H. (2019), "Razrabotka ontolohyy povedenyia vzymodeistvuiushchykh ahentov v systemakh bezopasnosty" [Development of an ontology of behavior of co-acting agents in security systems], *4th International Congresson 3DPrinting (Additive Manufacturing) Technologies and Digital Industry*, pp. 832-842.

14. Milov, O., Voitko, A., Husarova, I., Domaskin, O., Ivanchenko, E., Ivanchenko, I., Korol, O., Kots, H, Opirskyy, I. and Fraze-Frazenko, O. (2019), Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems, *Eastern-European Journal of Enterprise Technologies*, Vol. 9, No. 2, pp. 56-68.

15. Hryshuk, R. and Yevseiev, S. (2017), "Metodolohiia pobudovy systemy zabezpechennia informatsiinoi bezpeky bankivskoi informatsii v avtomatyzovanykh bankivskykh systemakh" [Methodology to encourage systems and security of information security in bank automation in automated banking systems], *Information security*, Vol. 23, No. 3, pp. 204-214.

16. Yudin, O.K. and Buchyk, S.S. (2015), "*Derzhavni informatsiini resursy. Metodolohiia pobudovy klasyfikatora zahroz*" [*State information resources. Methodology for building a threat classifier*], NAU, Kyiv.

17. Yudin, O.K., Buchyk, S.S., Chunarova, A.V. and Varchenko, O.I. (2014), "Metodolohiia pobudovy klasyfikatora zahroz derzhavnym informatsiinym resursam" [Methodology for building a threat classifier for public information resources], *Technology-intensive*, No. 2(22), pp. 200-210.

18. Yudin, O.K. and Buchyk, S.S. (2015), "Klasyfikatsiia zahroz derzhavnym informatsiinym resursam normatyvno-pravovoho spriamuvannia. Metodolohiia pobudovy klasyfikatora" [Classification of threats to state information resources of regulatory direction. Methodology for constructing the classifier], *Information security*, No. 17(2), pp. 108-116.

19. Buchyk, S.S. (2016), "Teoretychni osnovy analizu ryzykiv dereva identyfikatoriv derzhavnykh informatsiinykh resursiv" [Theoretical bases of analysis of risks of the tree of identifiers of state information resources], *Technology-intensive*, No. 1(29), pp. 70-77.

20. Buchyk, S.S. (2016), "Metodolohiia analizu ryzykiv dereva identyfikatoriv derzhavnykh informatsiinykh resursiv" [Methodology for analyzing the risks of the state information resource identifier tree], *Information security*, No. 1(18), pp. 81-89.

21. Domariev, D., Domariev, V. and Prokopenko, S. (2013), "Metodyka otsiniuvannia zakhyshchenosti informatsiinykh system za dopomohoiu SUSh "Matrytsia" [Methodology of Information Systems Security Assessment Using the Matrix School], *Information security*, Vol. 15, No. 1, pp. 80-86.

22. Pavlenko, S.V. (2009), "Metod otsinky zakhyshchenosti informatsiinykh system" [Method of estimation of information systems security], *Systems of Arms and Military Equipment*, No. 4(20), pp. 149-154.

23. Buchyk, S.S. (2015), "Metodyka ekspertnoho otsiniuvannia funktsionalnykh profiliv zahroz derzhavnykh informatsiinykh resursiv" [Methods of expert evaluation of functional profiles of threats to state information resources], *Open information and computer integrated technologies*, No. 70, pp. 271-280.

Список літератури

1. Грищук Р.В. Основи кібербезпеки / Р.В. Грищук, Ю.Г. Даник. – Житомир: ЖНАЕУ, 2016. – 636 с.

2. Євсеєв С.П. Класифікатор кіберзагроз інформаційних ресурсів автоматизованих банківських систем / С.П. Євсеєв // Кібербезпека: освіта, наука, техніка. – 2018. – № 2(2). – С. 47-67.

3. Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD [Electronic resource]. – 1985. – Available at: https://csTe.mst.gov/csTe/media/pubtications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf (accessed 7 December 2017).

4. Office for Official publications of the European Communities, Information Technology Security Evaluation. Criteria v. 1.2. [Electronic resource]. – 1991. – Available at: https://www.bsi.bund.de/SharodDocs/Dowrdoads/DE/BSrZertifizierung/ITSicherheitskriterien/itsec-enjxff.pdf?_blob=pubticationFile (accessed 7 December 2017).

5. Canadian System Security Centre, Communications Security Establishment. Canadian Trusted Computer Product Evaluation Criteria v. 3.0. [Electronic resource] / Government of Canada. – 1993. – Available at: http://www.btb.tenniurnplus.gc.ca/tpv2alpha/alphaeng.lrtml?lang=eng&i=&index=alt&srclrtxt=CANADIAN%20TRUSTED%20COMPUTER%20PRODUCT%20EV ALUATION%20CR1TERIA (accessed 7 December 2017).

6. US Government. Federal Criteria for Information Technology security [Electronic resource]. – NIST, NSA, US Government, 1993. – Available at: https://www.cotmnoncriteriaportal.org/files/ccfiles/ccpartlv2.3.pdf. (accessed 7 December 2017).

7. ISO/1EC 15408-1:1999. Information technology – Security techniques – Evaluation criteria for IT security – Part I: Introduction and general model [Electronic resource]. – Available at: https://www.iso.org/ni/standard/27632.html (accessed 7 December 2017).

8. ISO/1EC 15408-2:2005. Information technology – Security techniques – Evaluation criteria for ГТ security – Part 2: Security functional requirements [Electronic resource]. – Available at: https://www.iso.org/ru/standard/40613.html (accessed 7 December 2017).

9. ISO/IEC 15408-3:2008. Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements [Electronic resource]. – Available: https://www.iso.org/ru/standard/46413.html (accessed 7 December 2017).

10. CEM-97A)17. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model.

11. Горбенко И.Д. Критерии и методологии оценки безопасности информационных технологий [Электронный ресурс] / И.Д. Горбенко, А.В. Потий, П.И. Терещенко. – Режим доступа: http://www.bezpeka.com/ni/hb/spec/infsys/artl08.html.

12. Евсеев С. Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода / С. Евсеев // Інформаційна безпека. – 2017. – № 2(26). – С. 110-120.

13. Милов А.В. Разработка онтологии поведения взимодействующих агентов в системах безопасности / А.В. Милов, О.Г. Король // 4th International Congresson 3DPrinting (Additive Manufacturing) Technologies and Digital Industry 2019 (11-14 April, 2019). – P. 832-842.

14. Development of methodology for modeling the interaction of antagonistic agents in cybersecurity systems / O. Milov, A. Voitko, I. Husarova, O. Domaskin, E. Ivanchenko, I. Ivanchenko, O. Korol, H. Kots, I. Opirskyy, O. Fraze-Frazenko // Eastern-European Journal of Enterprise Technologies. – 2019. – Vol. 9, No. 2, P. 56-68.

15. Гришук Р. Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах / Р. Гришук, С. Євсеєв // Безпека інформації. – 2017. – Том 23, № 3. – С. 204-214.

16. Юдін О.К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз / О.К. Юдін, С.С. Бучик. – К: НАУ, 2015.

17. Методологія побудови класифікатора загроз державним інформаційним ресурсам / О.К. Юдін, С.С. Бучик, А.В. Чунарьова, О.І. Варченко // Наукоємні технології. – 2014. – № 2(22). – С. 200-210.

18. Юдін О.К. Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування. Методологія побудови класифікатора / О.К. Юдін, С.С. Бучик // Захист інформації. – 2015. –Том 17 (2). – С. 108-116.

19. Бучик С.С. Теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С.С. Бучик // Наукоємні технології. – 2016. – № 1(29). – С. 70-77.

20. Бучик С.С. Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С.С. Бучик // Захист інформації. – 2016. – № 1(18). – С. 81-89.

21. Домарєв Д. Методика оцінювання захищеності інформаційних систем за допомогою СУШ "Матриця" / Д. Домарєв, В. Домарєв, С. Прокопенко // Захист інформації. – 2013. – Том 15, № 1. – С. 80-86.

22. Павленко С.В. Метод оцінки захищеності інформаційних систем / С.В. Павленко // Системи озброєння і військова техніка. – 2009. – № 4(20). – С. 149-154.

23. Бучик С.С. Методика експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів / С.С. Бучик // Открытые информационные и компьютерные интегрированные технологии. – 2015. – № 70. – С. 271-280.

Received by Editorial Board 2.10.2018
Signed for printing 19.11.2019

Відомості про авторів:

Мілов Олександр Васильович
кандидат технічних наук доцент
доцент кафедри
Харківського національного економічного
університету ім. С. Кузнеця,
https://orcid.org/0000-0001-6135-2120

Мілевський Станіслав Валерійович
кандидат економічних наук доцент
доцент кафедри
Харківського національного економічного
університету ім. С. Кузнеця,
https://orcid.org/0000-0001-5087-7036

Король Ольга Григорівна
кандидат технічних наук доцент
доцент кафедри
Харківського національного економічного
університету ім. С. Кузнеця,
https://orcid.org/0000-0002-8733-9984

Information about the authors:

Oleksandr Milov
PhD in Technical Sciences Associated Professor
Senior Lecturer of Department of S. Kuznets
Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0001-6135-2120

Stanislav Milevskyi
PhD in Economics Associated Professor
Senior Lecturer of Department of S. Kuznets
Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0001-5087-7036

Olha Korol
PhD in Technical Sciences Associated Professor
Senior Lecturer of Department of S. Kuznets
Kharkiv National University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-8733-9984

РОЗРОБКА ВДОСКОНАЛЕНОГО КЛАСИФІКАТОРА ПОГРОЗ ДЛЯ МОДЕЛЕЙ ПОВЕДІНКИ АГЕНТІВ СИСТЕМ БЕЗПЕКИ

О.В. Мілов, С.В. Мілевський, О.Г. Король

Сучасний розвиток високих технологій та обчислювальної техніки справило значний вплив на розвиток систем управління бізнес-процесами, що охоплюють всі сфери економічної діяльності держави. Однак паралельно з цим ера високих технологій значно розширила спектр загроз, спрямованих на контур бізнес-процесів, і. перш за все, на інформаційні ресурси, що забезпечують функціонування контуру бізнес-процесів. При цьому загрози набули ознак гибридности і синергізму. У цих умовах актуальним питанням при формуванні системи управління інформаційною безпекою контуру бізнес-процесу є своєчасне виявлення і подальший аналіз сучасних загроз. В роботі представлені визначення контурів бізнес-процесів системи, що захищається і системи безпеки, наведені формальні описи відповідних контурів бізнес-процесів і взаємодії між ними. З метою узагальнення підходу класифікації гібридних кіберзагроз на складові безпеки: інформаційної безпеки (ІБ), кібербезпека (КБ), безпеку інформації (БІ) контуру бізнес-процесів і їх інформаційних ресурсів в роботі пропонується удосконалений класифікатор загроз контуру бізнес-процесів і забезпечують його інформаційних ресурсів , що включає вартісні оцінки реалізації загроз і оцінки втрат, пов'язаних з погрозами. Пропоновані розширення класифікатора загроз дозволяють реалізувати алгоритм визначення імовірнісних оцінок реалізації тих чи інших загроз, виходячи з доцільності їх проведення зловмисником, а також дати економічну оцінку доцільності захисту ресурсів від відповідної атак. На основі проведеного аналізу підходів пропонуються оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів в умовах дії сучасних гібридних кіберзагроз.

Ключові слова: *інформаційні ресурси; інформаційна безпека; гібридні кіберзагрози; контур бізнес-процесів; класифікатор загроз.*

РАЗРАБОТКА УСОВЕРШЕНСТВОВАННОГО КЛАССИФИКАТОРА УГРОЗ ДЛЯ МОДЕЛЕЙ ПОВЕДЕНИЯ АГЕНТОВ СИСТЕМ БЕЗОПАСНОСТИ

А.В. Милов, С.В. Милевский, О.Г. Король

Современное развитие высоких технологий и вычислительной техники оказало значительное влияние на развитие систем управления бизнес-процессами, охватывающих все сферы экономической деятельности государства. Однако параллельно с этим эра высоких технологий значительно расширила спектр угроз, направленных на контур бизнес-процессов, и. прежде всего, на информационные ресурсы, обеспечивающие функционирование контура бизнес-процессов. При этом угрозы приобрели признаки гибридности и синергизма. В этих условиях актуальным вопросом при формировании системы управления информационной безопасностью контура бизнес-процесса является своевременное выявление и последующий анализ современных угроз. С целью обобщения подхода классификации гибридных киберугроз на составляющие безопасности: информационной безопасности (ИБ), кибербезопасность (КБ), безопасность информации (БИ) контура бизнес-процессов и их информационных ресурсов в работе предлагается усовершенствованный классификатор угроз контуру бизнес-процессов и обеспечивающих его информационных ресурсов, включающий стоимостные оценки реализации угроз и оценки потерь, связанных с угрозами. Предлагаемые расширения классификатора угроз позволяют дать вероятностные оценки реализации тех или иных угроз. На основе проведенного анализа подходов предлагаются оценки показателей степени опасности злоумышленников и степени реализации защитных мер в условиях действия современных гибридных киберугроз.

Ключевые слова: *информационные ресурсы; информационная безопасность; гибридные киберугрозы; контур бизнес-процессов; классификатор угроз.*