INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT

UDC 00.004 https://doi.org/10.23947/1992-5980-2020-20-2-178-187

Algorithm of software package of intellectual decision support when designing cyber security system at the enterprise

E. A. Vitenburg, A. V. Nikishova
Volgograd State University (Volgograd, Russian Federation)

Introduction. To increase the decision-making efficiency at the enterprise, it is advisable to use a special software package of intellectual support. Such a product is necessary when designing an information security system and increasing its invulnerability during modernization or configuration changes. Research objectives are as follows: to develop an algorithm and a mathematical model of the software package for intellectual decision support.

Materials and Methods. The decision support method under designing an information security system is based on the use of a neural network (multilayer perceptron). For an objective assessment of the initial security of an information system (IS), a mathematical model for the analysis of security events is developed.

Results. The statistics of malicious attacks on the IS of enterprises is analyzed. The need for timely and accurate modernization of the information protection system is determined. Important characteristics of the designing an information security system are the speed at which the result is obtained and the reduction in the residual risk of IS. In this regard, the use of artificial intelligence systems in the process of determining the best set of protection subsystems is important. The threats to cyber security (CS) are classified. The main classes of security events are defined. A mathematical model of the neural network is developed; the input parameters of its operation are indicated. The current enterprise IS generates numerous events which necessitates the automatic collection and analysis of data from subsystems for registering IS objects. The process of analyzing security events is considered in detail since the adequacy of the generated design decisions depends on the correctness of the data obtained in this way. The algorithm of the software package is formed.

Discussion and Conclusions. The results can be used in the design of the information security system at the enterprise. In addition, CS administrators can use the developed software package to adjust the configuration settings of information security tools. The proposed solution will minimize the destructive influence of the developer of the security system which may and happen to be subjective.

***Keywords**:* cyber security, information system, neural network engineering, multilayer perceptron, algorithm.

For citation: E. A. Vitenburg, A. V. Nikishova. Algorithm of software package of intellectual decision support when designing cyber security system at the enterprise. Vestnik of DSTU, 2020, vol. 20, no. 2, pp. 178—187. https://doi.org/10.23947/1992-5980-2020-20-2-178-187

***Funding information*:** the research is done with the financial support of young Russian scientists from the Grants Council of President of the Russian Federation in R&D on “Building a model of intellectual decision-making support when designing an information security system at the enterprise”.

Introduction. With the development of industry in Russia, the number of enterprises classified as objects of critical information infrastructure (OCII) is growing. Statistics on the distribution of attacks from the Positive Technologies[1] vendor shows an increase in the number of successfully implemented malicious actions in this area. In 2019, 125 attacks on industrial information systems (IS) were recorded. This is more than three times (or by 212%) higher than the same indicator in 2018 (40 attacks). The diagram of the distribution of the number of attacks by quarters of the year (Q) is shown in Fig. 1.

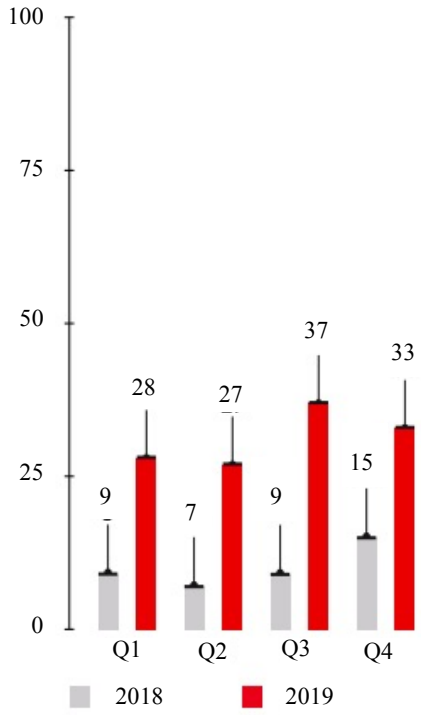

Fig. 1. Number of attacks on IS of enterprises in 2018 and 2019

Industrial IS are attacked mainly using malicious software (90% of attacks). This area is supervised by the Federal Security Service and the Federal Service for Technical and Expert Control. The need to ensure cyber security (CS) of industrial information systems is confirmed by statistics of the head research centers [1]. According to the regulatory legal acts of the Russian Federation[2], the owners of the OCII use a set of organizational and technical measures to ensure the safe operation of the information infrastructure. At the same time, the legislation provides for a periodic audit of the information protection system (IPS) performance, an assessment of its effectiveness. This results in prompt updating of the configuration settings of available tools or the retrofitting of the system with information security tools. A special role is played by the efficiency and accuracy of the decisions made, and the value of residual risk should not exceed the established indicators [2]. In this regard, it is proposed to automate the decision support process under designing the IPS at the enterprise.

Materials and Methods. To support decision-making in the design of IPS, a method based on a neural network (multilayer perceptron) was used [3]. Input data for the operation of a neural network were information security threats and security events. In addition, for an objective assessment of the initial information system security, a mathematical model of the analysis of security events was developed. Within this model, the calcu-

[1]Aktual'nye kiberugrozy: IV kvartal 2019 goda [Current cyber threats: Q4, 2019]. Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q4 (accessed 24.02.2020).
[2]O bezopasnosti kriticheskoi informatsionnoi infrastruktury RF: feder. zakon ot 26.07.2017, № 187-FZ [On security of critical information infrastructure of the Russian Federation: Federal Law of July 26, 2017, no. 187-FZ]. RF State Duma, Federation Council. FSTEC of Russia. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (accessed 18.05.20).

lated measures of IS similarity are compared with one of the IS security levels. Weighted Manhattan Distance is used as a similarity metric.

Study Results. In the framework of this study, an approach to the design of a protection system based on the factors of the cyber security subsystem importance included in the IPS [4] is proposed. With these data, it is suggested to make a list of security tools for the most critical subsystems. This approach provides strengthening the IPS through neutralizing critical threats. Moreover, criticality should be specified through an automated analysis of security events [5, 6]. The vector of cyber security subsystem importance is generated according to the expression

$$V = S(Class\_Thr), \tag{1}$$

where $V = (V_1, \dots, V_9)$ is the vector of IPS subsystem importance; $Class\_Thr = (Class\_Thr_1, \dots, Class\_Thr_6)$ is the vector of criticality of threat classes; S is the functional relationship defined by a neural network.

For convenience, we divide set of CS threats Thr into classes $Class\_Thr$, which are defined as in [6]:

$$Class\_Thr = \{Thr\_Br, Thr\_L, Th\_Dist, Thr\_Loss, Thr\_B, Thr\_A\}, \tag{2}$$

where Thr_Br is the class of CS threats of the "cracking" type; Thr_L is the class of CS threats of the "leak" type; Th_Dist the class of CS threats of the "distortion" type; Thr_Loss is the class of CS threats of the "loss" type; Thr_B is the class of CS threats of the "blocking" type; Thr_A is the class of CS threats of the "abuse" type.

To generate the vector of IS CS threat criticality, it is proposed to form two matrices of compliance:

— set of threats to set of classes of threats — $MThr$,

— set of security events to threat classes — $MEvent$.

$MThr$ matrix:

$$MThr = Thr \times Class\_Thr = (mth_{ij}). \tag{3}$$

Here, mth_{ij} is determined from the formula:

$$mth_{ij} = \begin{cases} \frac{1}{n}, \text{if the threat belongs to the threat class,} \\ 0 \text{ if not.} \end{cases} \tag{4}$$

Here, n is the number of threat classes to which the threat belongs.

In this case, $\forall i, \sum_j mth_{ij} = 1$.

$MEvent$ matrix:

$$MEvent = Events \times CThr = (mev_{ij}). \tag{5}$$

Here, mev_{ij} is determined from the formula:

$$mev_{ij} = \begin{cases} 1, \text{if an event occurs when a class threat is implemented,} \\ 0 \text{ if not.} \end{cases} \tag{6}$$

To form the vector of the cyber security subsystem importance, it is proposed to use a neural network in a software package — a multilayer perceptron operating according to the formula given in [7]:

$$\begin{cases} In_{0k} = v_k \\ Out_{ij} = f(\sum_l w_{ijl} In_{ijl} - \theta_{ij}), \\ In_{ijl} = Out_{i-1l} \end{cases} \tag{7}$$

where In_{0k} is the k-th neuron of the input layer; v_k is the k-th element of the input vector; Out_{ij} is the output value of the j-th neuron of the i-th layer; f is the neuron activation function, which is determined by the functional dependence V (1); w_{ijl} is the weight of the l-th input of the j-th neuron of the i-th layer; In_{ijl} is the value of the l-th input of the j-th neuron of the i-th layer; θ_{ij} is the activation level of the j-th neuron of the i-th layer; Out_{i-1l} is the output value of the l-th neuron of the $(i-1)$-th layer.

At the stage of analyzing security events, the initial data are the security event logs created by the system and the application software of the enterprise IS. Set of the security *Events* include the following classes [8]:

$$Events = \{EnterEv, ManagementSubEv, AccessObjEv, PolicyChangeEv,$$

$$Events = \{EnterEv, ManagementSubEv, AccessObjEv, PolicyChangeEv,$$

$$UsePrivilegesEv, ISProcessesEv, LevelISEv\}. \quad (8)$$

Here, $EnterEv$ are events of the "subjects' log-on" class; $ManagementSubEv$ are events of the "subject management" class; $AccessObjEv$ are events of the "accessing objects" class; $PolicyChangeEv$ are events of the "system policy change" class; $UsePrivilegesEv$ are events of the "subject's using exclusive privileges" class; $ISProcessesEv$ are events of the "system processes running" class; $LevelISEv$ are events of the "system level" class.

Dangerous events are selected from the set. Matrices of compliance are used to compare the set of dangerous events to threat classes. The matrix developed in the framework of this study is presented in Table 1.

Table 1

Matrix of compliance of CS threats of enterprise IS

Security event class	Threat types						
	$EnterEv$	$ManagementSubEv$	$AccessObjEv$	$PolicyChangeEv$	$UsePrivilegesEv$	$ISProcessesEv$	$LevelISEv$
Thr_Br	+		+		+		
Thr_L			+			+	
Th_Dist	+					+	
Thr_Loss			+			+	
Thr_B		+					+
Thr_A	+	+		+	+		+

Then the vector of urgent threat classes of CS IS threats is developed. After that, the subsystems of IPS are opposed to the urgent threat classes. Compliance is determined using a neural network with account for the functional dependence *V* in accordance with the formula (1).

Quite an important factor is the number of analyzed sets of events and their sources. It should be noted that the number of security events is directly proportional to the number of sources — information resources of the enterprise IS [8]. Given a large number of events generated by a working IS, it is valid to automatically collect and analyze data from the registration subsystems of IS objects that describe events. In this regard, it is worth considering in detail the analysis of security events since the adequacy of the generated design decisions depends on the correctness of the conclusions received at this stage.

According to [9, 10], at a given instant *T*, the current state of the enterprise IS $S_T \in State, State = \{Snorm, Sdang, Sanorm\}$ can be characterized as:

— normal ($Snorm$) — normal system operation in accordance with its tasks and as given in the documents regulating the work;

— dangerous ($Sdang$) — incorrect IS operation, when malfunctions associated with hacker attacks, crashes and failures of software and (or) hardware are recorded;

— abnormal ($Sanorm$) — temporary change in the normal IS operating mode and a surge in abnormal activity of users, programs and network traffic.

Dangerous and abnormal events require a more detailed analysis. A set of such events is the input to the stage of matching threat classes. Such events indicate the implementation of security threats.

Therefore, the results of monitoring and analysis of security events will be the input to the neural network (7).

Any $EventIS_i$ security event can be described by an attribute tuple [9]:

$$EventIS_i = \langle ID, Data, Level, Source, EventType, EventState, SecureParams \rangle, \quad (9)$$

где *ID* is the event ID; *Data* is the event generation time; *Level* is hazard level of the event; *Source* is the source of the event; *EventType* is the event type; *EventState* is event status; *SecureParams* is event security parameter vector.

$$SecureParams = \langle h, u, risk \rangle, \quad (10)$$

where h is an indicator for the generation of the event of a certain code relative to the total number of security events over the period ΔT; u is the severity of the consequences of the event (potential damage); *risk* is the IS information security risk.

Over the period ΔT, a set of IS events (*EventIS*) which should be evaluated to determine the level of IS security is generated in the information system.

The ratio of the number of events of one type or another to the total number is determined by the indicator h:

$$h = \frac{NEventID}{NEvent}, \quad (11)$$

where *NEvenID* is the number of events of a certain code, *NEvent* is the total number of events over the period ΔT.

The application software defines event codes differently. So, in the framework of this work, we have considered the encoding of the Windows OS Microsoft[3].

The IS information security risk is a function of the frequency of the event and the potential damage:

$$risk = h \times u. \quad (12)$$

The sum of private indicators determines the overall risk $RiskSum$:

$$RiskSum = \sum_{i=1}^{EventID} risk_i. \quad (13)$$

The set that provides the classification of events and the assessment of private indicators of IS security is described by subsets of elements:

$$PPS = \{\{EvType\}, \{EvState\}, \{ISState\}\}. \quad (14)$$

Here, *EvType is* a set of types of the events detected; *EvState is* a set of possible event states:

$$EvState = \{Ev^n, Ev^d, Ev^a\}, \quad (15)$$

where Ev^n — events of normal IS operation; Ev^d — IS CS threat events; Ev^a— abnormal events characterizing deviations of the IS from the normal mode of operation (additional analysis is needed).

To determine whether event $EventIS_i$ belongs to one of the three states *EvState*, the classification problem is solved — the set $SP = DamgeEv \cup NormEv$ is used, which is divided into two basic subsets. They are formed by an expert group on the basis of data on quick events of the normal IS operating mode and the previously detected CS attacks and incidents that describe the signature of IS quick and threat events:

— $DamgeEv$ is a set of events that are known features of an attack or determine the scenario of an incident;

— $NormEv$ is a set of events typical for the normal mode of IS operation.

[3]Opisanie sobytii sistemy bezopasnosti v Windows 7 i Windows Server 2008 R2 [Description of Security Events in Windows 7 and Windows Server 2008 R2]. Microsoft. URL: https://support.microsoft.com/ru-ru/help/977519/description-of-security-events-in-windows-7-and-in-windows-server-2008 (accessed 05.08.2019).

$F(EventIS_i(EvState) \to \{SP\}_j)$ are classified as follows:

$$EventIS_i(EvState) = \begin{cases} Ev^n, EventIS_i \in NormEv, \\ Ev^d, EventIS_i \in DamageEv, \\ Ev^a, EventIS_i \notin NormEv \cup DamageEv. \end{cases} \quad (16)$$

Here, $EventIS_i(EvState)$ are IS events with a status attribute, each of which corresponds to a set of connections SP_j with quick events from a set of templates of the normal mode and the mode with CS breach.

If the event is not present in the profiles of quick events or security breach events, it is determined to be abnormal. The reasons for its occurrence should be considered separately by the administrator of the IS system.

ISState ={*ISnorm, ISdang,ISanorm*} *is* a set of IS statuses indicating a normal mode of IS operation. The IS status is determined from the formula:

$$ISState = \begin{cases} ISnorm, \forall EventIS_i \in EventIS | EvState = Ev^n, \\ ISdang, \exists EventIS_i \in EventIS | EvState_i = Ev^d, \\ ISanorm, ISnorm \cap ISdang, \end{cases} \quad (17)$$

where *ISnorm* is the mode of normal IS operation; *ISanorm* is the mode of IS operation with features of abnormal activity; *ISdang* is the mode with fixed IS security breaches (Fig. 2).

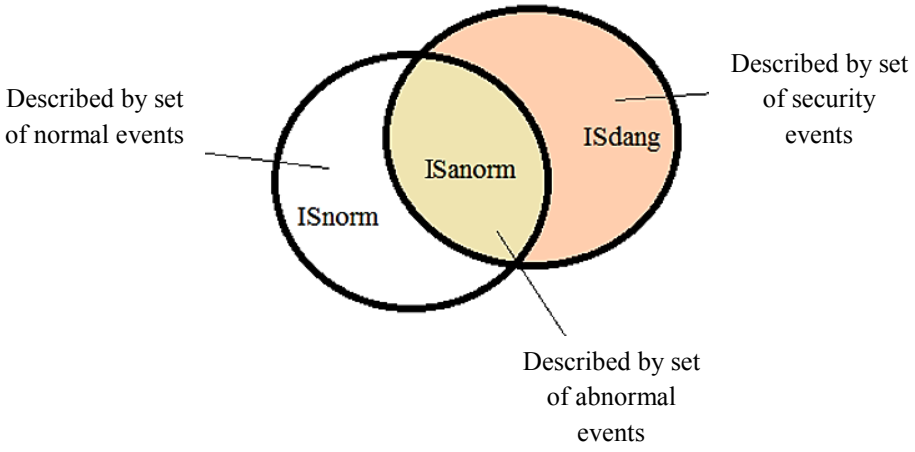

Fig. 2. Relationships of subsets of IS states

Based on the data obtained, a vector is formed that determines the IS status, the total risk, as well as the proportion of abnormal and security breaches:

$$IS = \langle ISState, RISKsum, NanalEv, NdandEv \rangle, \quad (18)$$

where $NanalEv$ is the proportion of detected abnormal events, $NdandEv$ is the proportion of events of CS breach of the enterprise IS.

To make a decision on whether to strengthen information security subsystems, the IS security level *SL* is calculated:

$$SL = \{\text{safe, stable, abnormal, crisis, dangerous}\}.$$

To determine the level of IS security, the designer of the CS system generates a vector that defines the reference indicator of the IS security IS_Perf. SL is formed according to the similarity of vectors *IS* and IS_Perf.

Five levels are accepted for evaluating the IS security within the framework of this mathematical model; therefore, when determining whether the IS belongs to one of the levels, the *k*-nearest neighbor method is used [10]. To this end, intermediate vectors corresponding to the remaining four security levels are compiled.

This operation is based on the values of the IS_Perf vector corresponding to the safe level of the IS status when multiplied by a scalar correction factor (the value is determined by experiment):

$$k \times RIS = \langle k \times ISState, k \times RISKsum, k \times NanalEvent, k \times\times\ NdandEvent \rangle. \quad (19)$$

Weighted Manhattan distance is used as a similarity metric [10]:

$$\rho(IS, RIS) = w \sum_{j=1}^{4} |IS_j - RIS_j|. \quad (20)$$

Based on the presented mathematical model, a generalized algorithm for the operation of a software prototype has been developed (Fig. 3).

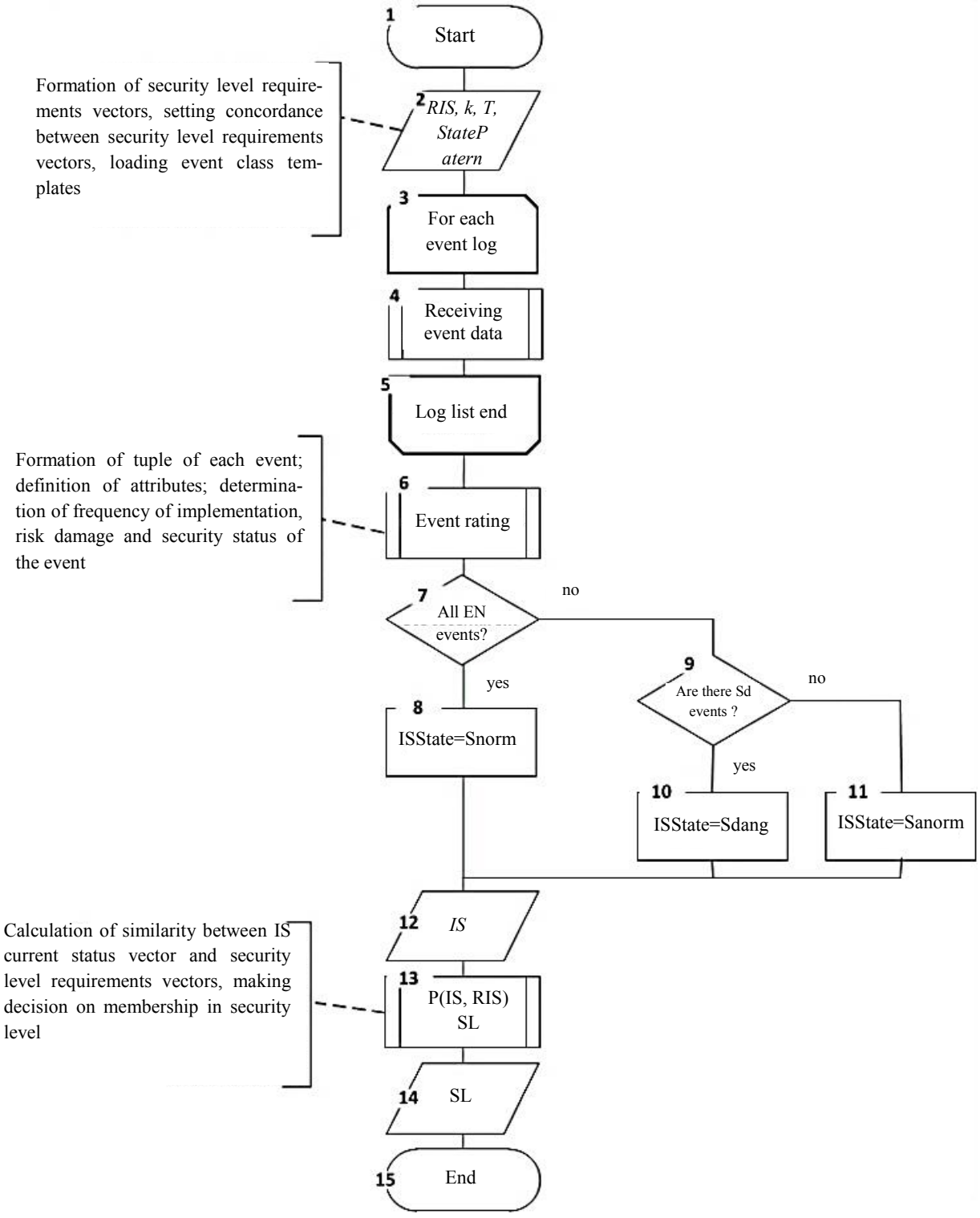

Fig. 3. Algorithm for software prototype of decision smartness complex when designing an information security system at the enterprise

Step 1 (blocks 1, 2). Launching a software prototype. The algorithm start. Input of data on the requirements vectors IS_Perf to the IS status of each security level. Enter the period over which monitoring will be conducted. Loading from the DB templates with sets of normal and dangerous events.

Step 2 (blocks 3–5). Monitoring OS event logs, receiving records on each event. Event listing.

Step 3 (block 6). Data analysis of the collected events, formation of the event tuple — the formula (8). Classification of events according to the formulas (14–15) into normal, abnormal, and dangerous ones. Calculation of the frequency of occurrence of events, potential damage and risk using the formulas (11–13).

Step 4 (blocks 7–11). Classification of IS states according to the formula (17) based on the event distribution data into a set of abnormal, normal, and dangerous ones (step 3).

Step 5 (blocks 12–14). Based on the calculated data and event tuple in the IS, the formation of the current status vector, calculation of similarity between IS and IS_Perf vectors: the formulas (19), (20). Decision-making on whether IS belongs to one of the five security levels.

Step 6 (block 15). The algorithm completion.

Discussion and Conclusion. In the framework of this study, an approach to modeling an information security system is proposed. Different qualitative and quantitative complex of security tools is taken into account depending on the actual threats to information security breaches. The presented method provides increasing the efficiency of the introduced cyber security system and reduces the likelihood of a designer mistake. The software package developed as part of this study has advantages that cannot be obtained under “manual” design:

- accounting of all data on the protected system,
- obtaining accurate results at the earliest.

References

1. Maiorova EV. Metodicheskie aspekty reagirovaniya na intsidenty informatsionnoi bezopasnosti v usloviyakh tsifrovoi ehkonomiki [Methodological aspects of responding to information security incidents in the digital economy]. Saint-Petersburg Economic Journal. 2020;1. URL: https://cyberleninka.ru/article/n/metodicheskie-aspekty-reagirovaniya-na-intsidenty-informatsionnoy-bezopasnosti-v-usloviyah-tsifrovoy-ekonomiki (accessed 24.02.2020). (In Russ.)

2. Bratchenko AI, Butusov IV, Kobelyan AM, et al. Primenenie metodov teorii nechetkikh mnozhestv k otsenke riskov na-rusheniya kriticheski vazhnykh svoistv zashchishchaemykh resursov avtomatizirovannykh sistem upravleniya [Application of methods of theory of fuzzy sets to assess the risk of violations of critical properties protected resources automated control system]. Cybersecurity Issues. 2019;1(29). URL: https://cyberleninka.ru/article/n/primenenie-metodov-teorii-nechetkih-mnozhestv-k-otsenke-riskov-narusheniya-kriticheski-vazhnyh-svoystv-zaschischaemyh-resursov (accessed: 24.04.2020). (In Russ.)

3. Vitenburg EA. Matematicheskaya model' intellektual'noi podderzhki prinyatiya reshenii pri proektirovanii sistemy zashchity informatsii na predpriyatii [Mathematical model of intellectual decision support when designing an enterprise information security system]. In: Industrial Automatic Control Systems and Controllers. Moscow: Nauchtekhlitizdat; 2019. P. 54–60. (In Russ.)

4. Vitenburg EA, Levtsova AA. Vybor ehlementov kompleksa zashchity informatsionnoi sistemy predpriyatiya na osnove trebovanii normativno-pravovykh dokumentov [Selecting safety package components

of enterprise information system following requirements of standard legal documents]. Vestnik of DSTU. 2018;3:333–338. (In Russ.)

5. Stepanova ES, Mashkina IV, Vasil'ev VI. Razrabotka modeli ugroz na osnove postroeniya nechetkoi kognitivnoi karty dlya chislennoi otsenki riska narusheniya informatsionnoi bezopasnosti [Development of threats model on the basis of fuzzy cognitive maps contraction for information risk numerical estimation]. Izvestiya SFedU. Engineering Sciences. 2010;11(112):31–40. URL: https://cyberleninka.ru/article/n/razrabotka-modeli-ugroz-na-osnove-postroeniya-nechetkoy-kognitivnoy-karty-dlya-chislennoy-otsenki-riska-narusheniya-informatsionnoy (accessed 24.04.2020). (In Russ.)

6. Vitenburg EA, Levtsova AA. Model' ugroz informatsionnoi sistemy predpriyatiya [Model of threats of enterprise information system]. Industrial Automatic Control Systems and Controllers. 2018;9:46–50. (In Russ.)

7. Bova VV, Dukkart AN. Primenenie iskusstvennykh neironnykh setei dlya kollektivnogo resheniya intellektual'nykh zadach [Application of artificial neural networks for collective decision of complex intelligent problems]. Izvestiya SFedU. Engineering Sciences. 2012;7(132):131–138. (In Russ.)

8. Smolyak DS, Pulko TA. Monitoring sobytii informatsionnoi bezopasnosti tekhnogennykh ob"ektov [Monitoring of information security events of technogenic objects]. In: Reports of the Belarusian State University of Informatics and Radioelectronics. Minsk: BSUIR Publ. House; 2015. P. 43–47. (In Russ.)

9. Mashkina IV, Sentsova AYu, Guzairov MN, et al. Ispol'zovanie metodov sistemnogo analiza dlya resheniya problemy obespecheniya bezopasnosti sovremennykh informatsionnykh sistem [Use of system analysis methods for the solution of information protection problem of information systems]. Izvestiya SFedU. Engineering Sciences. 2011;12(125):25–35. (In Russ.)

10. Astrakhov AV, Klimov SM, Sychev MP. Protivodeistvie komp'yuternym atakam. Tekhnologicheskie osnovy [Countering computer attacks. Technological basis]. Moscow: Bauman University Publ. House; 2013. 70 p. URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-techno.pdf (accessed 18.05.2020). (In Russ.)

Submitted 27.03.2020
Scheduled in the issue 27.04.2020

About the authors:

Vitenburg, Ekaterina A., postgraduate student of the Information Security Department, Volgograd State University (100, Universitetskiy pr., Volgograd, 400062, RF), ResearcherID: N- O-8740-2017, ScopusID 57209346586, ORCID: https://orcid.org/0000-0002-1534-8865, e.vitenburg@ec-rs.ru

Nikishova, Arina V., associate professor of the Information Security Department, Volgograd State University (100, Universitetskiy pr., Volgograd, 400062, RF), Cand.Sci. (Eng.), ResearcherID: N-3217-2016, ScopusID 57201358403, ORCID: https://orcid.org/0000-0002-0919-2593, nikishova.arina@volsu.ru

Claimed contributorship

E. A. Vitenburg: basic concept formulation; research objectives and tasks setting; creation of a mathematical apparatus for processing security events; formulation of conclusions. A. V. Nikishova: academic advising; analysis of the research; development of a mathematical apparatus of intellectual decision support; correction of the conclusions.

All authors have read and approved the final manuscript.