Intelligent decision support for information protection system’s design

E A Vitenburg¹, A V Nikishova¹, M Yu Umnitsyn¹ and T A Omelchenko¹
¹Volgograd State University, 100 prospect Universitetskii, Volgograd, 400062, Russia
E-mail: nikishova.arina@volsu.ru

Abstract. The article defines the need to protect enterprise information systems. To ensure the security of enterprise information system, depending on the stage of a life cycle, it is necessary to design, control and upgrade the information protection system. We propose the approach to designing enterprise information system’s protection based on the method of intelligent decision support, which uses a neural network. To do so we form the mathematical model of intelligent decision support for designing of enterprise information system’s protection. It takes into account the data of monitoring and analysis of security events.

1. Introduction
The development of information technologies in the modern world allows not only to minimize human labor expenditures, but also to optimize the production process and to establish full control over it. Modern industry started using information technology relatively recently. Integration of industrial systems and corporate systems provided users with extensive opportunities to maintain technological and support processes in the enterprise. However, from the information security point of view enterprise information systems have become less isolated, which has led to an increase in various kinds of malicious attacks. This factor determines necessitates of the timely design of an effective protection system.

The variety of protection subsystems that can be used to protect against several types of threats and the territorial distribution of enterprise information system’s components complicates the task of selecting a set of protection subsystems that form a protection system.

The choice of protection subsystems can be carried out several times during the life cycle of information system. Thus the important characteristics of the selection process are the speed of result’s reception, and the reduction of the residual risk.

Therefore, it is important to use artificial intelligence systems in selection for the best set of protection subsystems. It is important to take into consideration that information protection system’s forming can be carried out at different stages of an enterprise information system’s life cycle. Also the formation of an effective existing information protection system should take into account the statistics of information security incidents that occurred at the enterprise in recent years, as well as forecasted indicators.

The international standard ISO 27001:2013 [1] points out the need to apply a procedure for information security incidents’ managing. Since without timely response to information security incidents, eliminating their consequences and possible causes, it is impossible to effectively manage information security. Therefore, the actual direction of countering modern security incidents in information systems is the creation and application of security monitoring and management systems.
Their functions are monitoring and correlation of security events, security control, timely detection of unauthorized changes and their consequences, as well as decision support for design or modification of information protection system.

The main theoretical and practical aspects of the problem of information security monitoring and management systems’ creation are explored in the works of modern Russian scientists and specialists: Tsaregorodtsev A.V. [2], Makarevich O.B. [3], Zefirov S.L. [4], Astakhova L.V. [5], Livshits I.I. [6], Vasilyev V.I. [7], Bedran A. [8], Kotenko I.V. [9] and others. The analysis of these scientists’ works shows that research in this area can be divided into several groups:

- creation and improvement of security events’ data collection and correlation;
- security events’ analysis for attacks’ detection;
- methods’ development for risk assessment and security events’ ranking in order to identify and predict information security incidents and timely form an effective information protection system;
- methods’ development for countermeasures’ selection based on the analysis of information security events and incidents;
- development of new and improvement of existing algorithms for decision support in information security management and/or security system’s design.

At present leading vendors in the field of information security offer a wide range of software products for security events’ monitoring and analyzing [10]. Events monitoring and analysis tools are provided by the following software: MaxPatrol SIEM, HP ArcSight, Security Capsule SIEM, IBM Qradar. Each of these programs has a number of advantages and disadvantages. MaxPatrol SIEM, developed by Russian company Positive Technologies, as well as Security Capsule SIEM, developed in Russia by “ITB”, has a certificate of conformity of FSTEC of Russia on the level of control of undocumented features absence. In addition, MaxPatrol SIEM and Security Capsule SIEM provide the use of a large number of connectors, which allows to receive and analyze events from various sources. Unlike their foreign counterparts, HP ArcSight and IBM Qradar, MaxPatrol SIEM and Security Capsule SIEM provide file and software integrity control.

As a result, each software presents a detailed report on the events’ analysis to the user [10]. Based on this report, the user can make a conclusion about the security degree and absence of incidents in the information system. If the user observes signs of attack’s implementation or occurrence of information security incident in the report, he can make the decision on correction of protective measures. So he can strengthen the information system’s protection and counter the malicious effect.

The decision process, in this case, depends entirely on the decision-maker. Especially it depends on his level of professionalism as the information security specialist, his subjective views on the process of information security ensuring, and psycho-emotional component. In addition, from the beginning of attack’s identification to the protection measures’ application, a long period of time can pass. And so the decisions aimed at providing protection against a particular malicious impact will be taken untimely.

This problem can be eliminated if the decision process is automated. However, nowadays in the field of information security there are no ready-made software solutions that allow not only to monitor and analyze security events, but also to generate management solutions aimed at enterprise information system’s protection improvement based on security events’ analysis. These management solutions can include changing in information protection system’s structure or correction of protection tools’ settings.

A large number of works on security events’ monitoring and decision models based on monitoring data for information protection system’s design shows relevance and necessity of this research. The purpose of the research is to automate the process of information protection system’s design and/or modifying taking into account data of security events’ monitoring and analysis.
2. Proposed approach
We propose a design methodology that takes into account security events generated by the existing enterprise information system. This allows the information security specialist to use exactly those protection means that belong to the most important protection subsystems. These means allow protecting against the most relevant classes of threats. To calculate the importance of information protection subsystems we use formula (1):

\[ I = N (A), \]  

where \( I = (I_1, \ldots, I_9) \) – vector of information protection subsystems’ importance; \( A = (A_1, \ldots, A_6) \) – vector of threat classes relevance; \( N \) – functional dependence represented by a neural network.

Moreover, in order to determine the vector of threat classes relevance based on security events’ monitoring data, we define two compliance matrices:

1) matrix \( M_{\text{Th}} \) of compliance between a set of threats \( \text{Thr} \) and a set of threat classes \( \text{CTh} \). \( M_{\text{Th}} = \text{Thr} \times \text{CTh} = (m_{th_{ij}}) \), where

\[ m_{th_{ij}} = \begin{cases} 1, & \text{if threat belongs to threat class} \\ 0, & \text{otherwise} \end{cases} \]  

where \( n \) – number of threat classes. Meanwhile \( \forall i, \sum m_{th_{ij}} = 1. \)

2) matrix \( M_{\text{Ev}} \) of compliance between a set of security events \( \text{Ev} \) and a set of threat classes \( \text{CTh} \). \( M_{\text{Ev}} = \text{Ev} \times \text{CTh} = (m_{ev_{ij}}) \), where

\[ m_{ev_{ij}} = \begin{cases} 1, & \text{if event occur during implementation of threat of class} \\ 0, & \text{otherwise} \end{cases} \]  

The used neural network is a multilayer perceptron, which functions according to (4).

\[
\begin{align*}
\text{In}_{0k} &= v_k \\
\text{Out}_{ij} &= f(\sum_i \omega_{ij} \text{In}_{ijl} - \theta_{ij}) \\
\text{In}_{ijl} &= \text{Out}_{i-1l}
\end{align*}
\]

where \( \text{In}_{0k} \) – the \( k \)-th neuron in the input layer; \( v_k \) – the \( k \)-th element of the input vector; \( \text{Out}_{ij} \) – the output value of the \( j \)-th neuron of the \( i \)-th layer; \( f \) – activation function of the neuron; \( \omega_{ij} \) – the weight of \( l \)-th entry of the \( j \)-th neuron of the \( i \)-th layer; \( \text{In}_{ijl} \) – value of \( l \)-th entry of the \( j \)-th neuron of the \( i \)-th layer; \( \theta_{ij} \) – the activation level of the \( j \)-th neuron of the \( i \)-th layer; \( \text{Out}_{i-1l} \) – output value \( l \)-th neuron of \((i-1)\)-th layer.

So we present the functional model of information protection subsystems’ intellectual selection as following (figure 1).

The inputs to the security event analysis phase are the event sets generated by the enterprise information system. We use the classification of security events proposed by MicroSoft in this research [11]. The set of security events includes the following types (5):

\[ \text{Events} = \{ \text{EnterEv}, \text{ManagementSubEv}, \text{AccessObjEv}, \text{PolicyChangeEv}, \text{UsePrivilegesEv}, \text{ISPProcesseEv}, \text{LevelISEv} \}. \]  

where EnterEv – set of events of “account logon” type; ManagementSubEv – set of events of “account management” type; AccessObjEv – set of events of “object access” type; PolicyChangeEv – set of events of “policy change” type; UsePrivilegesEv – set of events of “privilege use” type; ISPProcesseEv – set of events of “process tracking” type; LevelISEv – set of events of “system” type.

We selected dangerous events from a variety of security events. We also mapped dangerous security events to threat classes using compliance matrixes. As a result, we determined the vector of relevance of threat classes. We use a neural network to determine the compliance between the relevance of threat classes and the importance of information security subsystems.
Comparison with threat classes
Determining importance of information protection subsystem
Relevance of security event classes

Relevance of threat classes

Security event monitoring

Figure 1. Intellectual choice of information protection subsystems

It is worth considering the fact that the number of event sources increases with the growth of the number of users, servers, workstations and software and hardware elements of enterprise information system and/or reconfiguration of enterprise information system. Taking into account a large number of events generated by enterprise information system during its functioning, it is important to conduct automatic collection and analysis of events’ data from the registration subsystems of information system’s objects. In this regard, we gave the most detailed consideration of the stage of security events’ analysis. Because the correctness of the conclusions obtained during this stage affects the correctness of the generated design decisions.

According to the result of sources’ [12-14] analysis, we determined that the current state of the enterprise information system – $S_T$ at a certain time $T$, $S_T \in \text{State}$, $\text{State}=\{\text{Snorm}, \text{Sdang}, \text{Sanorm}\}$ can belong to one of three possible types:

- normal $\text{Snorm}$ – regular functioning of information system in accordance with its tasks and according to the documents regulating its work;
- dangerous $\text{Sdang}$ – normal functioning is disrupted, violations of information system’s functioning associated with attacks, failures of software and/or hardware of information system occurs;
- abnormal $\text{Sanorm}$ – characterized by a temporary change in the normal mode of information system’s functioning and a surge of abnormal activity of users, software and network traffic.

We described each distinguished type of information system’s state by its own set of events and parameters, which according to the states we also divided into normal, dangerous and abnormal events.

Events related to dangerous events and anomalous events require more detailed analysis. The set of such events is the input data of the threat class comparison stage. These events indicate the implementation of security threats.

Since the methods of attacks’ implementing can change over time, it is more convenient to operate with classes of threats of information security violations for the purposes of scientific research [15].
The set of threats of information security violation Threat can be conveniently divided into classes CTh, which we defined in the formula (6).

\[
\text{Threat} = \{\text{Breaking}, \text{Leak}, \text{Distortion}, \text{Loss}, \text{Blocking}, \text{Abuse}\}, \tag{6}
\]

where Breaking – set of threats that fall into the “breaking” category, Leak – set of threats that fall into the “leakage” category, Distortion – set of threats that fall into the “distortion” category, Loss – set of threats that fall into the “loss” category, Blocking – set of threats that fall into the “blocking” category, Abuse – set of threats that fall into the “abuse” category.

Then the mapping of threats’ classes and security events’ classes we defined as in table 1.

### Table 1. Compliance of threats’ classes and security events’ classes

| Threats’ class                  | Security events’ class                                    |
|--------------------------------|----------------------------------------------------------|
| Threats of breaking category   | Events of object access type                             |
| Threats of leakage category    | Events of object access type; events of process tracking type |
| Threats of distortion category | Events of object access type; events of process tracking type; events of system type |
| Threats of loss category       | Events of system type; events of privilege use type      |
| Threats of blocking category   | Events of account logon type                             |
| Threats of abuse category      | Events of account management type; events of privilege use type; events of policy change type |

Therefore, the input data for the neural network is:

- results of enterprise information system’s events’ monitoring – MIS;
- classification of events and evaluation of information system’s private security indicators.

Data about each event EventISi are collected from the log during monitoring of information system within the specified time interval $\Delta T$. These events form a set of information system’s events EventIS and are assessed. We use corsette (7) to describe event attributes.

\[
\text{EventISi} = (\text{ID}, \text{Date}, \text{Level}, \text{Source}, \text{EventType}, \text{EventState}, \text{SecureParams}), \tag{7}
\]

where ID – event’s code; Date – time and date of event’s occurrence; Level – event’s level; Source – event’s source; EventType – event’s type; EventState – event’s state; SecureParams – vector of event’s security parameters (8).

\[
\text{SecureParams} = (h, u, \text{risk}), \tag{8}
\]

where $h$ – frequency of event’s occurrence; $u$ – potential damage of event’s consequences; risk – amount of information security risk of the event.

We determine the frequency of event’s occurrence $h$ by the ratio of the number of events of certain code to the total number of events within the specified time interval $\Delta T$ (9).

\[
h = \frac{\text{NEventID}}{\text{NEvent}}, \tag{9}
\]

where NEventID – number of events of certain code; NEvent – total number of events within the specified time interval $\Delta T$.

The potential damage of event’s consequences $u$ depends on the value level of each event Level and we describe it by a quantitative – qualitative scale of levels (table 2).

We calculate information security risk of each event, which is a function of frequency of event’s occurrence and potential damage of event’s consequences, by the formula (10).
risk=h*u. \hspace{1cm} (10)

We calculate the total risk RiskSum for all events as the sum of the private risks according to (11).

\[ RiskSum = \sum_{i=1}^{EventID} risk_i. \] \hspace{1cm} (11)

| Potential damage u | Value level of event Level |
|---------------------|-----------------------------|
| u=0 low             | Information                  |
| u=3 medium          | Warning                      |
| u=6 high            | Mistake                      |
| u=10 critical       | Critical error               |

We describe the set that provides classification of events and estimation of private security indicators by subsets of elements (12).

\[ \text{ACE} = \{ \text{EventType}, \{ \text{EventState}, \{ \text{ISState} \} \} \}, \] \hspace{1cm} (12)

where EventType – set of detected events’ types; EventState – set of possible events’ states EventState=\{ Sn, Sd, Sa \}={0;1;0,5}, where Sn – normal events that are characteristic for the normal mode of enterprise information system’s functioning; Sd – dangerous events that are characteristic for enterprise information system where security breach (attack or security incident) is located; Sa – abnormal events characterizing deviations of information system from the normal mode of functioning. These events need additional analysis.

We reduced the process of determining whether an event EventIS, belongs to one of the three states to solving the classification problem. For this purpose we use the set StatePatern=DamgeEventUNormEvent. We divide the set into two basic subsets which are formed by an expert group based on data on typical events of normal enterprise information system’s functioning and previously detected information system attacks and incidents. So we formed the template or signature of events typical for this information system and dangerous events:

- set of typical security breach events DamgeEvent includes events that are known signs of an attack or are included in the events describing the scenario of a security incident;
- set of events NormEvent typical for information system’s normal functioning.
We implement classification $F(\text{EventIS}(\text{EventState}) \rightarrow \{\text{StatePatern}\})$ as in (13) (figure 2):

$$
\text{EventIS}_i(\text{EventState}) = \begin{cases} 
S^n, & \text{EventIS}_i \in \text{NormEvent} \\
S^d, & \text{EventIS}_i \in \text{DamageEvent} \\
S^a, & \text{EventIS}_i \notin \text{NormEvent} \cup \text{DamageEvent}
\end{cases}
$$

where EventIS$(\text{EventState})$ – information system’s events with state attribute, each of which corresponds to a set of relationships StatePatern, with typical events from sets of events of normal functioning and security breach.

Thus, if such an event is not in the template of known regular events or security breach events, it is considered abnormal and may indicate abnormal activity, caused either by the actions of an attacker, or a temporary authorized deviation from the normal mode of functioning.

At the second stage according to table 1 we carry out the comparison of detected dangerous events $\text{DamageEvent}$ to the set of threats defined in the formula (6).

And then the structure of information protection subsystems corresponding to the identified relevant classes of threats is automatically proposed.

3. Results and Discussion

On the basis of the proposed model, we developed software that allows both designers of information protection systems and information security specialists at the enterprise to form the most optimal set of information security tools – projects.

A screen copy of the results of software for intelligent decision support for information protection system’s design functioning is shown in figures 3-4.
Implementation of proposed projects increases the efficiency of information protection system in comparison with the process of information protection system’s design without decision support tools. This conclusion follows from the fact that the design will take into account the whole set of data about the protected system, which is difficult in “manual” design [16].

4. Conclusion
It’s important to note that developed software minimizes the subjective factors included in the design process by the protection system’s developer. Such factors include mistakes of the developer in the analysis of initial data, short terms of modernization and/or development of protection system, taking into account a large amount of information about the protected system, the inability to carry out a deep and comprehensive analysis of security event logs or statistics in a short time.

The application of the developed software allows designing optimal protection for a particular information system, taking into account the peculiarities of its functioning and its relevant threats.

Acknowledgment
The reported study was funded by the Council for grants of Russian Federation President, according to the research project No. MK-6404.2018.9.

References
[1] Sokolov S S, Alimov O M, Golubeva M G, Burlov V G and Vikhrov N M 2018 *IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)* 5 124–7
[2] TSaregorodtsev A V 2009 *Methods, Models and Algorithms of Synthesis of Protected Information Systems* (Moscow: Tax Academy of the Russian Federation Press) p 208
[3] Makarevich O B and Sheludko I A 2003 *Izvestiya SFedU. Engineering Sciences* 4 211–6
[4] Zefirov S L and Shcherbakova A IU 2014 *TUSUR Reports* 2(32) 77–81
[5] Astakhova L V and Tsimbol V I 2016 * Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics* 16(1) 165–9
[6] Livshits I I and Lontsikh P A 2015 *IrSTU Bulletin* 98(3) 268–73
[7] Vasilev V I, Pestrikov V A and Krasko A S *Izvestiya SFedU. Engineering Sciences* 8 7–14
[8] Bedran A 2009 *T–Comm — Telecommunications and Transport* 2 10–3
[9] Kotenko I V, Saenko I B and Iusupov R M 2014 *St.Petersburg State Polytechnical University Journal: Computer Science. Telecommunications and Control Systems* 198(3) 7–18
[10] Tarasenko N 2018 *SecurityLab.ru by Positive Technologies*
[11] Dwyer J and Truta T M 2013 9th *IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing* 9 563–70
[12] Mashkina I V, Sentsova A IU, Guzairov M N and Kladov V E 2011 *Izvestiya SFedU. Engineering Sciences* 125(12) 25–35
[13] Astrakhova L V, Klimov S M and Sychev M P 2013 *Countering Cyber Attack. Technological Base* (Moscow: BMSTU Press) p 70
[14] Kazimir V V and Seraia A A 2010 *Journal Mathematical Machines and Systems* 4 52–61
[15] Vitenburg E A, Pushikarskaia A I and Oladko V S 2017 *Information Systems and Technologies* 101(3) 21–30
[16] Vitenburg E A 2018 *Proc. of VolSU Scientific Session* (Volgograd: VolSU Publishing) pp 295–9