Probabilistic Analysis of the Influence of Staff Qualification and Information-Psychological Conditions on the Level of Systems Information Security

Igor Goncharov, Nikita Goncharov, Pavel Parinov,
Sergey Kochedykov and Alexander Dushkin

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.75079

Abstract

Taking into account the criticality of the "human factor," the probabilistic approach for analysis is proposed, including: a model for predicting and assessing the level of systems information security, considering random events, including dependent events; model of information-psychological impact on staff; methodical approach for analyzing an influence of staff qualifications and psychological conditions on the level of system information security. The effectiveness of the application is demonstrated by examples.

Keywords: human factor, information security, information-psychological impact, predicting, assessment

1. Introduction

Information systems are of high importance in organizations, industrial process, banking sector, etc. The "human factor" accounts for approximately 70% of information security breaches. Staff are one of the parts of information system. The influence of the "human factor" on the level of system information security is considered in various articles and standards. In particular, the international standards ISO/IEC 27002 provide recommendations for work with staff at various stages: prior to employment, during employment, termination, and change of employment [14]. The reliability of information system operation and the level of information security depend on different conditions. Wrong actions and inactivity of staff and untimely performance of job duties can lead to violations of integrity, availability, and confidentiality of the information. As a result they influence the level of system information security. The staff of information system have certain characteristics that affect a level of system information security as well as technical and software components. Such characteristics form mental state and psychophysical properties of staff. In addition to attacks on the information system implemented by technical methods, there is also an attack on the staff of the information system. This attack can be carried out by means of information-psychological impact (IPI). In this article, it is proposed to consider mathematical models for predicting and estimating the information security level of information systems, taking into account dependent events and information and psychological impact on staff, methods, and stages of implementing information and psychological impact. The approach to the analysis of staff conditions under the information-psychological impact is considered. A methodical approach is proposed for analyzing the impact of qualification and psychological states of staff on the information security level of the information system. The application of this model is considered.

2. Mathematical models for estimating the level of information security considering the impact of staff qualifications and psychological state

2.1. Model for predicting and assessing the level of systems information security considering dependent events

The boundaries of the conditions for the provision of procedures for modeling secure information systems in terms of compliance with integrity, availability, and confidentiality, and the information circulating in them [9, 12, 25] is estimated by the possibility of realizing their technical characteristics in real devices and conditions [2, 13, 15, 22, 23]. In particular, the ready-made nodes of known information systems are separate technical devices with characteristics corresponding with their passport data. They provide the possibility to choose the topology of the information system within the limits of the compatibility characteristics of the system nodes [2, 4, 13, 15, 22–24]. At the same time, consideration of this approach to modeling allows to choose the priority of providing information security criteria such as integrity, availability, and confidentiality, which are generally interdependent in the construction of an information system and analysis of the possibility of ensuring maximum levels of values of these criteria. It means that depending on the conditions, tasks, which should be solved, and the purpose of building and information system, first of all, it is more important to ensure integrity; second, if availability comes, then it is confidentiality or in another sequence.

This sequence may be due to the complexity of the information system, its configuration, the characteristics of the individual nodes, which are involved in its composition, and external factors that affect the operating conditions. The opinion of experts [12] who make decisions on estimating the values of the parameters of the safety criteria, based on an analysis of the physical characteristics of the information system under consideration, plays an important role in the implementation of this approach. The theorem on the multiplication of the probabilities of dependent events is at the heart of the approach for estimating the parameters of safety criteria [5]. This is due to the dependence of the safety criteria which is described above, estimated by mutual influence in the analysis of the characteristics of the information system. For example, a separate information system node is a complete single device with specific technical characteristics that are individually responsible for the likely conditions for ensuring either integrity or availability or confidentiality. At the same time, by virtue of the technical implementation, this node cannot be ideal from the point of view of safety criteria and cannot provide only either integrity or availability or confidentiality, since the information that must have a certain level of each criterion will circulate in it. And the characteristics of this node will extend to a certain part of the information system, which also estimates the important conditions for ensuring its security [26]. The security of information, in the sense of analyzing the probability of the existence of safety criteria, in the information system can be represented in the diagram of sets shown in **Figure 1**.

If the integrity (I), availability (A), and confidentiality (C) are separate sets, then security (S) is the intersection of these three sets.

It means that it is necessary to ensure both integrity, and availability, and confidentiality to a specific value of the appropriate criterion, estimated for each particular information system in order to ensure security [12, 25]. In its turn, from the point of view of ensuring the probability of the information system security and due to the interdependence described above, integrity, availability, and confidentiality are conditional signs. Then the probability of security should be considered in the following way (Eq. (1)) [12]:

$$p(\,Sec\,) = p(I \cap A \cap C). \tag{1}$$

The figure shows a graphical interpretation of the product of the corresponding events I, A, and C for which the following expression is valid (Eq. (2)):

$$p(I \cap A \cap C) = p(I) \cdot p_I(A) \cdot p_{IA}(C). \tag{2}$$

Since the events of ensuring integrity, availability, and confidentiality are dependent, then the probability of producing these events according to the multiplication rule for the probabilities of dependent events, is (Eq. (3)):

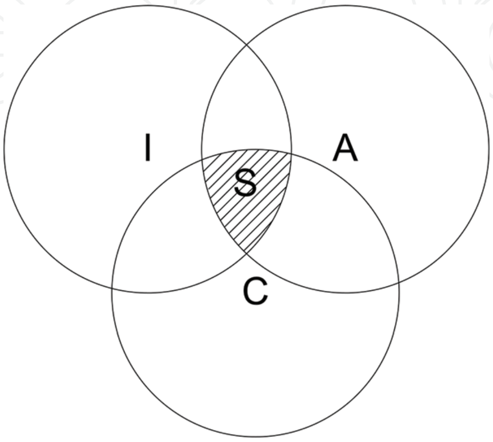

Figure 1. Presentation of integrity, availability, and confidentiality using sets.

$$p(I \cdot A \cdot C) = p(I) \cdot p(A/I) \cdot p(C/I \cdot A). \tag{3}$$

To describe the case, the probability of coexistence of several dependent events is equal to the product of the probabilities of these events, and the probability of each next event in the order of recording is calculated if all the previous ones also take place.

It means that the probability of ensuring both integrity and availability and confidentiality of information is equal to the product of the probability of ensuring integrity to the probability of providing availability if there is ensuring of integrity and the probability of ensuring of confidentiality while integrity and availability are provided.

As it was mentioned before, the priority of the place of writing in the formula of the corresponding probabilities can be estimated by the experts' opinion, taking into account the complexity of their calculation, caused by the need to implement the corresponding values of the safety criteria levels, according to the physical expressions which describe these criteria levels [12].

Thus, the described approach makes it possible to model various information systems based on real physical characteristics that allow to predict and evaluate the levels of safety criteria, taking into account the experts and experts' opinions, and it is actual and necessary in practical implementation nowadays [12]. The information security level of the information system can be estimated according to the calculated values (1).

2.2. Model of information-psychological impact on staff

Along with the impact on the technical and software components of the information system, there are also effects pointed to the staff of the information system (**Figure 2**). They are information-psychological impacts (IPI) [6–11]. They can lead to a change in the characteristics of employees that are the subject of IPI; as a result, the information security level of the information system may change. As a rule, IPI data are usually transmitted through common communication channels.

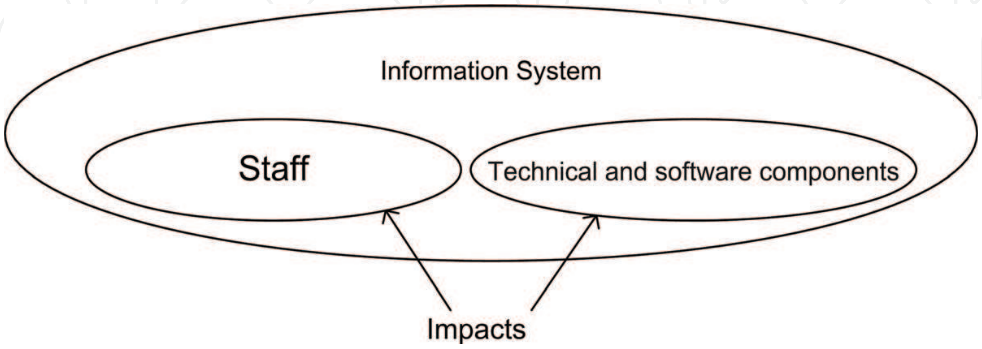

Figure 2. Impacts on the information system.

2.2.1. Stages of implementation of information and psychological impact

It is possible to single out the following stages of IPI implementation [6–11]:

1. The subject determines the goals to be achieved by IPI.
2. The subject determines the object of IPI.
3. The subject collects information about the IPI object and investigates the psychophysical characteristics of the IPI object in order to detect subject matters of the IPI object and their characteristics (the subject is understood to be a component of the IPI object that determines its possible characteristics; one characteristic may belong to several IPI objects).
4. The subject chooses the most appropriate means of influencing the IPI object and the communication channel, based on the data of points 1–3. Each of the means affects the relevant objects of influence and their characteristics.
5. The subject forms a message for the IPI object.
6. The subject implements an impact on the IPI object, with the aim of achieving a sustainable change in characteristics. To do it, the generated message is coded using the selected IPI tools and sent via the selected communication channel to the object.
7. The IPI object decodes the received message.
8. The decoded message affects the characteristics of the IPI object; as a result, they change, and there is some possibility of appearing/disappearing new characteristics.

In **Figure 3**, the scheme of IPI is shown.

2.2.2. Formal IPI model

The formal model of the IPI process is proposed [7, 8, 11]. For the IPI object *Obj* there is a set of subject matters Sub_i, and a set of characteristics (Eq. (4)) is defined for each of them:

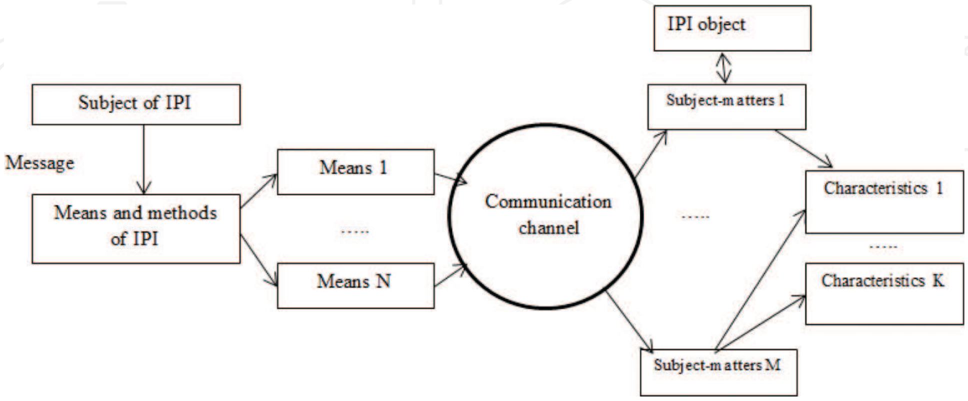

Figure 3. Scheme of IPI.

$$Obj = \{Sub_1, \dots, Sub_n\}, \;\; Sub_i = \{Char_1, \dots, Char_k\}. \tag{4}$$

Each object can have several characteristics. Dependence of objects and their characteristics is estimated in the matrix of properties. In the columns, the subject-matters of the IPI object are indicated; in the lines, characteristics are indicated; at the intersection, their correspondence is denoted (Eq. (5)):

$$Obj = \begin{pmatrix} Sub_1(Char_1) & Sub_2(Char_1) & \dots & Sub_n(Char_1) \\ Sub_1(Char_2) & 1 & \dots & Sub_n(Char_2) \\ \dots & \dots & \dots & \dots \\ 1 & Sub_2(Char_k) & \dots & Sub_n(Char_k) \end{pmatrix} \tag{5}$$

The subject has many means of impact that do not always correspond with articles of the IPI object; this is proposed that the set of means of the subject's impact is defined as $S = \{S_1, \dots, S_n\}$.

Each of the means of impact S_j is applied for the purpose of changing the property $Sub_i(Char_m)$ and affects different objects and their characteristics in different ways. The result of such a change will be denoted $Ef_{i,m,j}$, which can be equal to zero or be negative (that means it has the opposite effect to the aims of IPI) and can be positive (it means it can have an effect corresponding with the goals of the IPI).

Realization of IPI for m-characteristics (Eq. (6)):

$$\left(Sub_i(Char_m), S_j\right) = Ef_{i,m,j}. \tag{6}$$

For the case when the IPI object possesses articles with characteristics, and the subject has means of impact, this is proposed to obtain the matrix of efficiency of IPI; in the columns, the articles of the IPI object are indicated; in the lines, characteristics are indicated; at the intersection, their correspondence is denoted (Eq. (7)):

$$S = \begin{pmatrix} Ef_{1,1,1} & Ef_{1,1,2} & \cdots & Ef_{1,1,l} \\ Ef_{1,2,1} & Ef_{1,2,2} & \cdots & Ef_{1,2,l} \\ \cdots & \cdots & \cdots & \cdots \\ Ef_{n,1k1} & Ef_{n,k2} & \cdots & Ef_{n,k,l} \end{pmatrix}. \tag{7}$$

The sum of all impacts on the m-characteristic is described by Eq. (8):

$$\sum_{j=1}^{l} \left(Sub_i(Char_m), S_j\right) = Ef_{i,m}, \tag{8}$$

where the efficiency is provided when the matrixes are added in stages, which means that several IPI tools can affect one characteristic. The formal model of IPI implementation can be written in the following form (Eq. (9)):

$$(Obj, S) = \sum_{j=1}^{l} \begin{pmatrix} 1 & \dots & Sub_n(Char_1) \\ \dots & \dots & \dots \\ Sub_1(Char_k) & \dots & Sub_n(Char_k) \\ 1 & \dots & 1 \\ \dots & \dots & \dots \\ 1 & \dots & 1 \end{pmatrix} \cdot S_j, \quad Obj = \begin{pmatrix} 1 & \dots & Ef_{n,1} \\ \dots & \dots & \dots \\ Ef_{1,k} & \dots & Sub_n(Char_k) \\ 1 & \dots & Sub_n(Char_{k+1}) \\ \dots & \dots & \dots \\ Ef_{1,f} & \dots & 1 \end{pmatrix}. \tag{9}$$

Operation « · » has the following properties:

1. $Sub_i(Char_m) \cdot S_j = Ef_{i,m,j}$.

2. $Sub_i(Char_m) \cdot S_j = Ef_{i,m,j} = 1$—the property $Sub_i(Char_m)$ has disappeared.

3. $Sub_i(Char_m) \cdot S_j = Ef_{i,m,j} = 0$—the property $Sub_i(Char_m)$ has not changed.

$$1 \cdot S_j = \begin{cases} 1, \text{if the property continues being absent,} \\ Sub_s(Char_f), \text{if the property has appeared.} \end{cases} \tag{10}$$

The result of the malefactor's attack on the IPI object is a matrix of properties, which will take the changed form (Eq. (11)):

$$Obj = \begin{pmatrix} 1 & Ef_{1,2,l} & \dots & 1 \\ Ef_{2,1,j} & 1 & \dots & Sub_n(Char_2) \\ \dots & \dots & \dots & \dots \\ 1 & Sub_2(Char_k) & \dots & Sub_n(Char_k) \end{pmatrix}. \tag{11}$$

Some of the properties resulting from IPI may remain unchanged; others are replaced by $Ef_{i,m,j}$.

2.2.3. Mathematical model of information-psychological impact

The change in the property which undergoes IPI can be described by equation or model [11, 16–19] (Eq. (12)):

$$K = f(H, P), \tag{12}$$

where P is the characteristics of the IPI object, H is the characteristics of the IPI (means of impact), and K is the response (the level of change). As the characteristic of IPI, we will use H as the effectiveness of implementing the means of influencing the property $Ef_{i,m,j}$. Thus, the equation takes the form (Eq. (13)):

$$K = f((Obj, S), P). \tag{13}$$

Eq. (12) makes it possible to evaluate the change in the properties and the response of an object to IPI. In our case, staff are considered as the IPI object. Eq. (13) of the change in the property and the human reaction to the effects is given in articles [11, 16–19] and has the form (Eq. (14)):

$$R\frac{d^2Y}{dt^2}+\frac{2F\sqrt{RA}}{QF_0}\cdot\frac{dY}{dt}+\frac{A}{Q^2}Y=X, \tag{14}$$

where F is the frustration; F_0 means some value of the level of frustration, considered normal or threshold; A is the aggression; Q means the time parameter; R is the stiffness; X means the effectiveness of information-psychological impact; and Y is the reaction level. These parameters are measured in conditional scores. They can be estimated using psychological tests and an expert method. This is proposed to use Eq. (11) to estimate the change in the property of the IPI object as a result of the action. The transfer equation for Eq. (14) has the form (Eq. (15)):

$$W(p)=\frac{Q^2F_0}{RQ^2p^2F_0+2QF\sqrt{RA}p+AF_0}. \tag{15}$$

2.3. Methodological approach for analyzing the impact of staff qualifications and psychological conditions on the level of systems information security

Employees' qualifications, mental state, and psychophysical properties can act as their characteristics.

2.3.1. Staff qualification assessment

This is a proposed estimate of staff's qualification in an expert way:

- k = 0 if the staff of the information system are idle in the case of vulnerabilities, technical malfunctions are idle in the technical and software components of the information system [27, 28].
- k < 1 if the staff of the information system fail to remove vulnerabilities, technical malfunctions fail in the technical and software components of the information system in time [27, 28].
- k = 1 if the staff of the information system eliminate vulnerabilities, technical malfunctions eliminate in the technical and software components of the information system in time [27, 28].
- k > 1 if the staff of the information system independently detect and fix vulnerabilities (temporary solutions, before the release of the update from the manufacturer) in the technical and software components of the information system, technical malfunctions are prevented [27, 28].

The limiting minimum value for the staff's qualification k is 0, because staff does not create vulnerabilities and technical malfunctions in the technical and software components of the information system. The maximum value for the staff's qualification k is 3; in this case the security service includes a large number of highly skilled employees who can increase labor productivity working together.

The estimation should be carried out separately for each component because maintenance of various components of the information system is implemented in different ways. This is proposed to define the malfunction as various malfunctions in the operation of the information system components that require staff intervention to eliminate them. This is proposed to understand vulnerability as a defect of information system that can violate its integrity, availability, and confidentiality and cause a malfunction.

2.3.2. Impact of staff's psychological conditions on labor activity

During the work activity, the staff of the information system may be in different psychological conditions. The effectiveness of the staff depends on what psychological state they are in. The following states can be distinguished as [3, 20, 29]:

- Optimum working condition ensures the greatest efficiency of activity. It is characterized by the presence of a conscious goal of activity, high concentration of attention, aggravation of memory, and activation of thinking. The electroencephalogram shows that in this state, the brain rhythms mainly lie in the beta range.
- The state of tense activity arises in the course of work in abnormal situations. Mental tension develops directly in proportion to the difficulty of the task. Easy tasks are solved with minimal effort; complex and new actions require a higher degree of mental pressure. Mental tension is a physiological reaction of the organism, mobilizing its resources to perform more difficult tasks. Mental tension stimulates the physical and mental processes of the human body, which increases its adaptive abilities. The tension reaction develops in a responsible environment, as well as when people perform complex production tasks, if they change the stereotype of actions and habitat and if they are under the influence of extreme conditions. Under the influence of mental stress, vital body functions such as metabolism, circulation, and respiration change. If in the behavior of a person, there is some general concentration, the actions become clearer, the speed of motor reactions increases, and physical performance improves. At the same time, perception becomes aggravated, the process of thinking is accelerated, memory is improved, and concentration of attention is increased.

It should be remembered that the dependence of the efficiency of labor activity (working capacity) of employees on the level of tension of its functional systems is parabolic. It was found out that mental stress has a positive effect on the result of labor up to a certain limit. Exceeding the critical level of activation leads to a decrease in the results of labor up to a complete loss of efficiency.

- Fatigue is a functional state of a person, temporarily occurring under the influence of prolonged or intensive work, accompanied by a decrease in its effectiveness. Fatigue is caused by the depletion of body resources during prolonged or excessive activity and is characterized by a decrease in motivation to work, a violation of attention and memory.

At the physiological level, the appearance of a protective inhibition of the central nervous system is noted. Fatigue may eventually go into the exhaustion, which requires a longer rehabilitation to get it over.

- Stress is a state of increased and prolonged pressure associated with the inability to adapt to the requirements of the habitat. This condition is caused by the long-term impact of environmental factors, exceeding the possibilities of the organism adaptation. It is characterized by mental stress, a sense of frustration, anxiety, and worry, and in the last stage, indifference and apathy appear. At the physiological level, there is a depletion of adrenal hormone stores, muscle tension, and a two-phase activation of the autonomic nervous system.

Figure 4 shows the possible dynamics of staff states. The transition between states can occur both as a result of labor activity and under the influence of information-psychological impact.

The effectiveness of staff for different psychological conditions is a quantity with no dimension and can be estimated in the following way:

- For an optimal working condition, the efficiency of labor activity will be estimated as (Eq. (16)) [3, 20, 29]

$$E = k, \tag{16}$$

where k is the qualification of the staff.

- For the state of intense activity, the efficiency of labor activity will be estimated as (Eq. (17)) [3, 20, 29]

$$E = -at^2 + bt + k, \tag{17}$$

where *k* is the qualification of the staff, a [1/h^2] and b [1/h] are parameters that estimate the rate of staff fatigue, and t [h] is time.

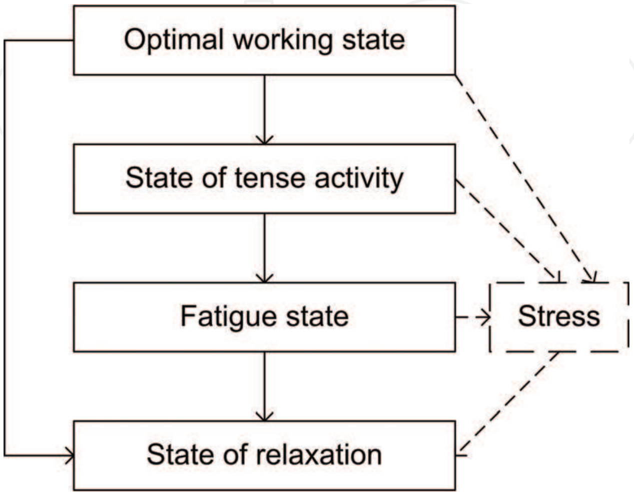

Figure 4. Possible dynamics of staff transitions in the course of labor activity.

- For the state of fatigue, the efficiency of labor activity will be estimated as (Eq. (18)) [3, 20, 29]

$$E = k - bt, \tag{18}$$

where k is the qualification of the staff, b [1/h] is the parameter that estimates the rate of staff fatigue, and t [h] is time.

- For the state of fatigue, the efficiency of labor activity will be estimated as (Eq. (19)) [3, 20, 29]

$$E = k - sbt, \tag{19}$$

where k is the qualification of the staff, b [1/h] is the parameter that estimates the rate of staff fatigue, s is the reaction to information-psychological impact, and t [h] is time.

- The efficiency of labor activity is equal to zero for the state of relaxation.

2.3.3. Mathematical model of information system operation

The information system consists of various technical and software components; each of them can have vulnerabilities and fail due to a technical malfunction. Vulnerabilities and technical faults pose a threat to the confidentiality, integrity, and availability of information. This is proposed to represent the information system as a set of queuing systems [26–28]; each of them simulates the dynamics of vulnerabilities and technical faults that threaten the confidentiality, integrity, and availability of information. The input of the described system receives a non-stationary Poisson stream of requests (vulnerabilities and faults). This model is presented in **Figure 5**, where $\lambda(t)$ is the speed of detection of vulnerabilities or faults that threaten the confidentiality, integrity, or availability of information; E is the effectiveness of staff to ensure the confidentiality, integrity, or availability of information; and T_a is the average time to eliminate the vulnerability or malfunction.

The average speed of elimination of vulnerabilities and faults of the information system will be described in the following way (Eq. (20)):

$$\mu = E\mu_a, \tag{20}$$

where μ_a is the average speed of elimination of the vulnerability and malfunction.

The assessment of μ_a will be estimated in the following way (Eq. (21)):

$$\mu_a = \frac{1}{T_a}. \tag{21}$$

The average number of vulnerabilities and faults in the information system will be the sum of the average number of vulnerabilities and faults that threaten the confidentiality, integrity, and availability of information (Eq. (22)):

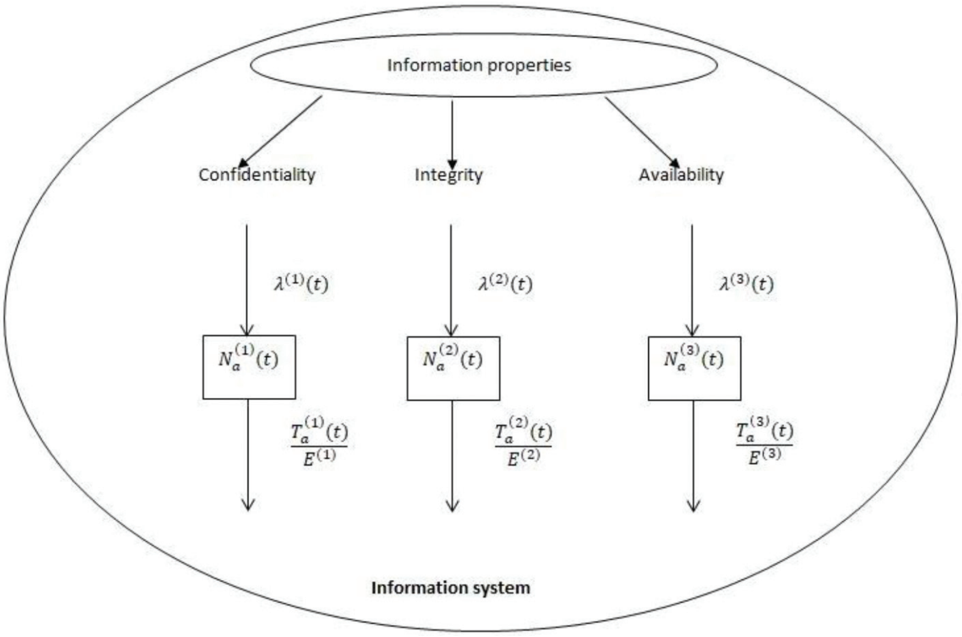

Figure 5. Model of changes in the state of security of the information system, taking into account the staff activities.

$$N_a(t) = \sum_{m=1}^{3} N_a^{(m)}, N_a^{(m)}(t) = \frac{T_a^m e^{-t}}{E^{(m)}} \left(\lambda^m(t) + \int_0^t \lambda^m(\tau) e^{\tau} d\tau \right). \tag{22}$$

When $E^{(m)}$ is equal to zero of vulnerability and faults, the average number of vulnerabilities and faults will be estimated as (Eq. (23))

$$N_a^{(m)}(t) = \int_0^t \lambda^m(\tau) e^{\tau} d\tau. \tag{23}$$

There is a probability of a number of vulnerabilities and faults (Eq. (24)):

$$P_n(t) = \frac{[N_a(t)]^n}{n!} e^{-N_a(t)}. \tag{24}$$

Thus, the probability of the absence of vulnerabilities and faults is (Eq. (25))

$$P_0(t) = e^{-N_a(t)}. \tag{25}$$

In general, based on the proposed models, it is proposed to estimate the security of the information system $P_{IS}(t)$, taking into account the impact of staff qualifications and psychological conditions, as (Eq. (26))

$$P_{IS}(t) = P_{Sec}(t) + P_0(t)(1 - P_{Sec}(t)), \tag{26}$$

where $P_{Sec}(t)$ is estimated from Eq. (3).

To analyze the influence of the human factor on the properties of each component of the investigated information system, one can consider, as (Eq. (27)) [1]:

$$\begin{aligned} P_I(t) &= P_I(t) + P_{0I}(t)(1 - P_I(t)), \\ P_A(t) &= P_A(t) + P_{0A}(t)(1 - P_A(t)), \\ P_C(t) &= P_C(t) + P_{0C}(t)(1 - P_C(t)), \end{aligned} \tag{27}$$

where $P_{0I}(t)$, $P_{0A}(t)$, and $P_{0C}(t)$ are the likelihood of the absence of vulnerabilities and faults in the component providing integrity, availability, and confidentiality.

3. Example of using models

Let us consider an information system, consisting of an X router and a file server under the management of the operating system Y. Users who are allowed to have an access connect to the router through a Wi-Fi connection and get an access to files according to the permitting access system.

In this information system, confidentiality, integrity, and availability are provided by means of a router and a server running the operating system Y.

It is possible to infringe the security of the information system by violating the performance of one of the components which are responsible for confidentiality, integrity, and availability.

As the experience of practical studies [12] has shown for 802.11 wireless networks in calculating the probability values of safety criteria, it is advisable to take noise immunity coding into account for the estimation of integrity. But it is necessary to take modulation efficiency and bandwidth usage technology into account for the estimation of availability, and it is important to take cryptographic strength of encryption into account for the estimation of confidentiality. Then the expression for the probability of ensuring the security of information takes the form (Eq. (28)):

$$p(\,Sec\,) = p(I) \cdot p(A/I) \cdot p(C/IA), \tag{28}$$

where

$$p(I) = p(coding\_immunity), \tag{29}$$

$$p(A) = p(Effect\_of\_\mathrm{modul}ar\_techno\log ical\_use\_of\_frequencies), \tag{30}$$

$$p(C) = p(cryptographic\_strenght\_of\_encryption), \tag{31}$$

With a more detailed representation of the parameters (Eq. (32)):

$$p(I) = p(r, R), \tag{32}$$

$$p(A) = p\big(S, SNR, V_m, p_{er}, parametr\_t\big), \tag{33}$$

$$p(C) = p\left(N, p_{\text{vu}\ln erability}, com\right), \tag{34}$$

where R is coding rate, r is relative redundancy of coding, S is spectral efficiency, SNR is a signal-to-noise ratio, V_m is modulation rate, C is the real throughput, p_{er} is the probability of a bit error, *parametr_t* is a parameter that estimates the effectiveness of the selected technology for the use of the frequency band, N is the number of possible combinations with the selected encryption (coding), $p_{\text{vu}\ln erability}$ is probability of the protocol's vulnerability, and *com* is password complexity. This makes it possible to choose the most flexible algorithm for modeling an information system with the required level of security [9].

Thus, perhaps there are five more options for writing and using the applied expression for multiplying dependent probabilities. Perhaps, because of the complexity of accounting for modeling the network with a great number of parameters in the above expressions, experts believe that in the proposed formula for calculating security, the probability of availability should be put on the first place, the second one should be given to the conditional probability of confidentiality, and then the conditional probability of integrity comes.

If it is possible to ensure security while ensuring integrity and confidentiality considering integrity and availability in the context of integrity and confidentiality, the expression for the probability of network security will take the following form (Eq. (35)):

$$p(\,Sec\,) = p(I) \cdot p(C/I) \cdot p(A/IC), \tag{35}$$

and so on.

Different variants of writing these expressions are fair to use then; it is more advantageous to calculate safety when taking into account the corresponding described conditions. For different networks, the probabilities of security criteria will be described by different physical expressions and different number of parameters in these physical expressions [5, 12].

For different information systems at different stages of the technological process that they implement, it may be expedient to differentiate the priority of providing information security criteria (integrity, availability, confidentiality), including the exclusion of some of them. For example, in information retrieval systems that provide users with a legislative basis or a database of threats, it is primarily necessary to ensure the integrity and availability of information, while ensuring confidentiality is not required, since information is publicly available.

Obtaining probability values is a separate research area and requires a separate assessment technique [12]. Values of the probability of ensuring integrity, availability, and confidentiality for various information systems are given in **Table 1**. These values are obtained on the basis of practical experience [21].

Table 2 shows the average time to resolve vulnerabilities and faults for components of various information systems.

Table 3 provides statistics on the intensity of vulnerability and fault detection for components of various information systems.

Let Obj_A (object IPI) be the staff possessing such things as Sub_1 which is the relation to any facts, events, phenomena, and members of a society [11]; Sub_2 is a mental state [11]; Sub_3 is the physiological state of the staff [11]. Things such as Sub_1, Sub_2, and Sub_3 have intersecting sets of properties (concentration, fatigue, understanding, emotionality, etc.).

Using Eq. (14), this is proposed to estimate the reaction to the information-psychological impact. Depending on the characteristics of the staff, the reaction can be both sustainable (staff can do their duties; their effectiveness is defined as Eq. (19)) and unstable (staff is incapable). In the case of an unstable reaction, the graph of the reaction level of the staff is periodic; in the case of a stable reaction, the graph of the reaction level of the staff will not be periodic. **Figure 6** presents examples of the dependence of the level of staff reaction on the information and psychological impact.

Let the staff in question have the following characteristics, obtained from the results of the psychological tests of Eysenck: $F = 16$, $F_0 = 10$, $A = 4$, and $R = 9$. Doing so, this is proposed to assume that the staff, being under the IPI, will not purposefully violate the technical and software components of the information system.

Using Eq. (26), this is proposed to estimate the probability of the security of the information system. **Figure 7a–c** shows the probability of the security of the information system, depending on the coefficient of staff work and their state, for the first, second, and third cases.

Probability $p(Sec)$	Availability	Confidentiality	Integrity
For Case 1	0.85	0.88	0.86
For Case 2	0.74	0.85	0.9
For Case 3	0.91	0.82	0.64

Table 1. Probabilities of ensuring integrity, availability, and confidentiality.

T_a	Availability	Confidentiality	Integrity
For Case 1	0.019	0.016	0.023
For Case 2	0.04	0.021	0.3
For Case 3	0.01	0.001	0.03

Table 2. Average time and speed of vulnerability and malfunction elimination.

λ	Availability	Confidentiality	Integrity
For Case 1	0.00366	0.002	0.0077
For Case 2	0.001	0.0047	0.01781
For Case 3	0.00146	0.0023	0.00724

Table 3. Statistics of the intensity of vulnerability and fault detection for components of the information system.

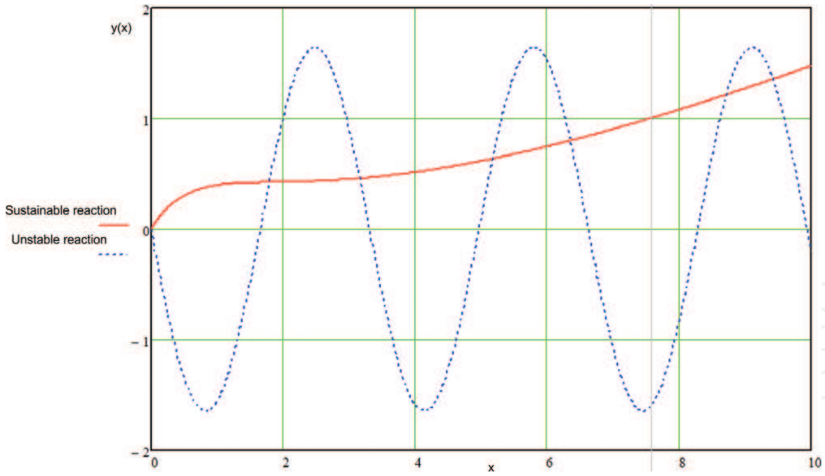

Figure 6. The level of the subject's reaction to information and psychological impact.

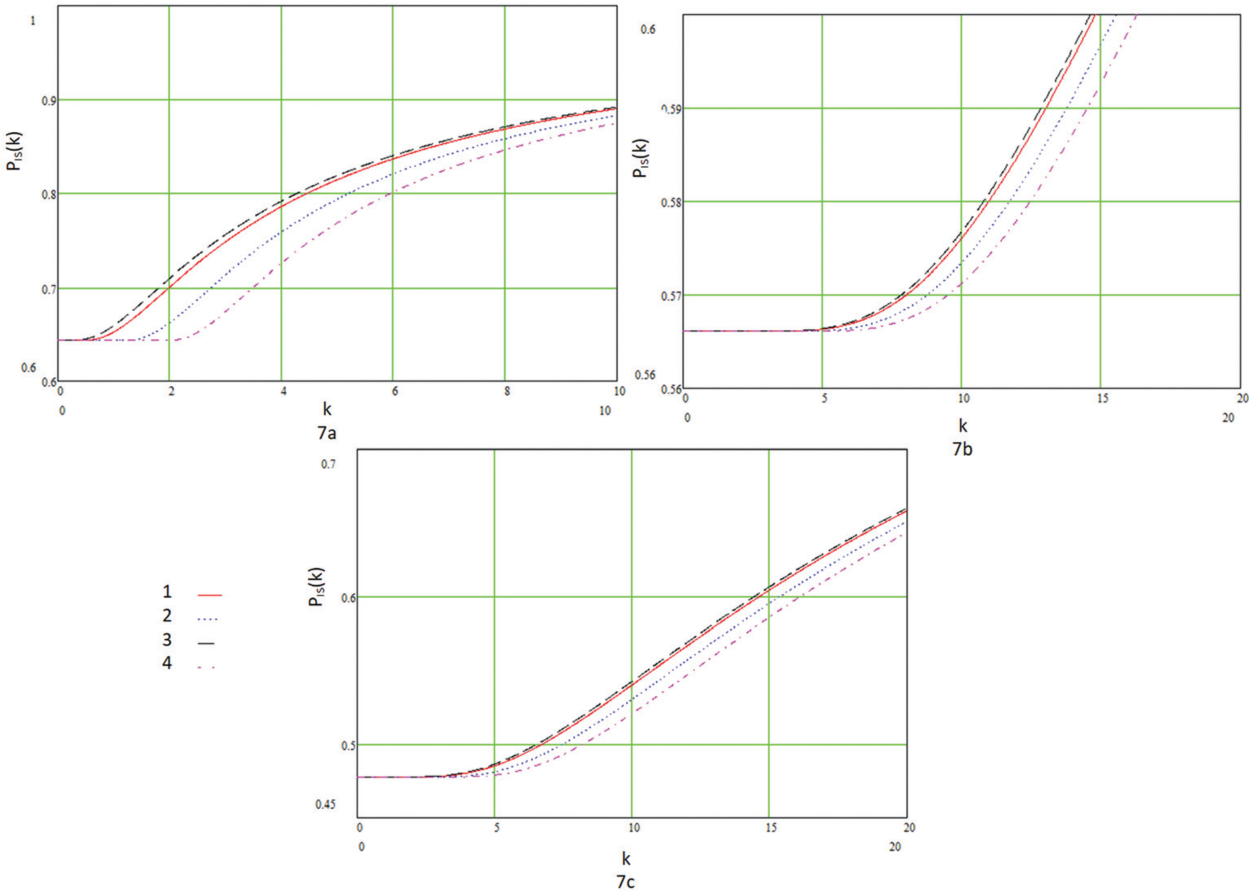

Figure 7. Probability of the information system security, depending on the employees' workload and their condition [(1) optimal condition, (2) fatigue status, (3) state of stressful activity, (4) stressful condition (impact on staff)].

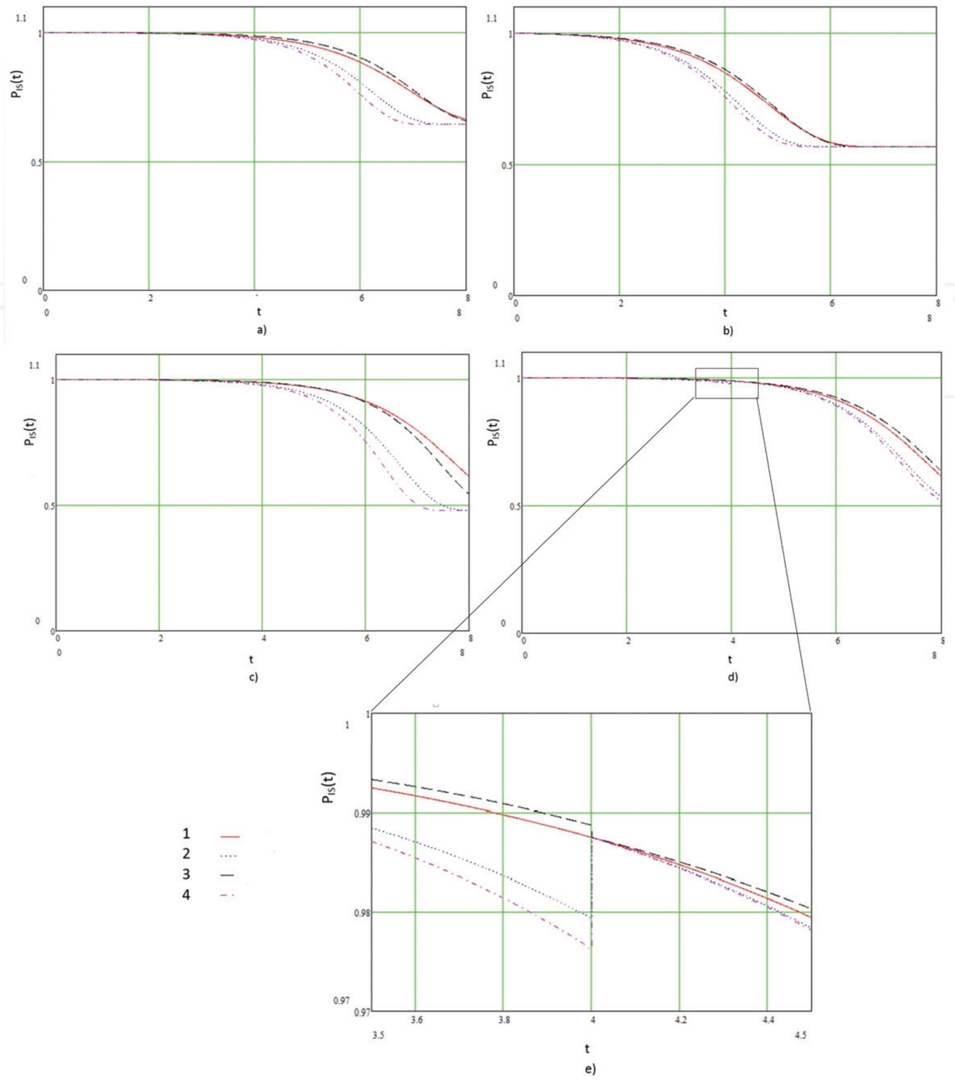

Figure 8. Probability of the information system security at the level of staff qualification is equal to 1, depending on the condition of the staff [(1) optimal condition, (2) state of fatigue, (3) state of tense activity, (4) stressful condition (impact on staff)].

At first, the results of IPI on staff are not apparent, so the graphics are depicted from 1 hour of the operation of the information system.

It can be seen from the graph that upgrading the skills of staff leads to an increase in the probability of security of the information system. Thus, the high qualification of the staff can compensate the information and psychological effects on the staff and their fatigue from prolonged activities.

Figure 8a–c shows the probability of security of the information system for the first, second, and third cases, respectively, if a staff qualification level is equal to one, depending on the condition of staff. **Figure 8d** shows the probability of the security of the information system for

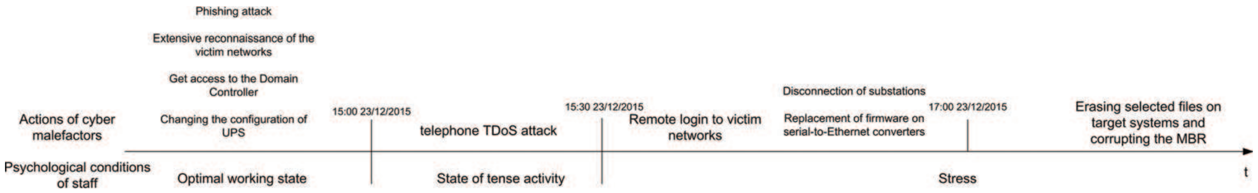
Phishing attack
Extensive reconnaissance of the victim networks
Get access to the Domain Controller
Changing the configuration of UPS
Actions of cyber malefactors
Psychological conditions of staff
Optimal working state
15:00 23/12/2015
telephone TDoS attack
State of tense activity
15:30 23/12/2015
Remote login to victim networks
Disconnection of substations
Replacement of firmware on serial-to-Ethernet converters
17:00 23/12/2015
Stress
Erasing selected files on target systems and corrupting the MBR
t

Figure 9. Time diagram of exemplary actions of cyber malefactors and psychological conditions of staff.

the third case, taking into account the recess for recovery. However, the time for the restoration process itself was not taken into account. **Figure 8e** shows an enlarged transition fragment after recovery for **Figure 8d**. A time interval equal to the average working day was taken for consideration.

At the initial stage of operation with a stressed state, the probability of ensuring the security of the information system is higher than at the optimal state, but this is a temporary effect; as it can be seen from **Figure 8a** with prolonged operation in the stressed state, the probability of the information system safety is lower than at the optimal state. With an optimal state, the probability of ensuring the security of the information system is higher than if staff are in a state of fatigue or under the influence of IPI in a stressful state. **Figure 8d** shows that if the staff use the break to restore their original characteristics, the probability of the information system safety increases.

For example, on December 23, 2015 [1], Ukrainian power companies experienced unscheduled power outages impacting a large number of customers in Ukraine. The outages experienced on December 23, 2015, were caused by external cyber attackers. After extensive reconnaissance of the victim networks, the telephone tdos attack was conducted on staff. As a result staff did not notice that substations disconnected in time. Exemplary actions of cyber malefactors and psychological conditions of staff are shown in the time diagram of **Figure 9**.

The received results coincide with the data obtained in the course of practical activity by interviewing the staff and owners of information systems, so it confirms the effectiveness of the proposed model for estimating the level of systems information security based on probabilistic analysis of the impact of their staff qualifications and psychological state.

Thus, to ensure the security of the information system, it is essential to take into account the abilities of staff. It is necessary to take into account the qualification of staff, which can change the probability of security of the information system characterized by technical and functional construction according to Eq. (1), from values $p(\mathit{Sec})$ to 1, to monitor the condition of the staff, keeping them in in an optimal working condition with breaks.

4. Conclusions

The proposed method allows to use the probabilistic assessment of the system information security, taking into account the technical characteristics of the components of the information system, the qualifications of the staff, the mental state of the employees, and their psychophysical characteristics. Their permanent use in system life cycle helps to increase information security and decrease a potential danger of "human factor."

Author details

Igor Goncharov[1]*, Nikita Goncharov[1], Pavel Parinov[1], Sergey Kochedykov[2] and Alexander Dushkin[2]

*Address all correspondence to: goncharov@infobez.org

1 JSC "NGO" Infosecurity, Voronezh, Russia

2 Voronezh Institute of the Federal Penitentiary Service of Russia, Voronezh, Russia

References

[1] Cyber-Attack Against Ukrainian Critical Infrastructure. Available form: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

[2] Deev V. Methods of modulation and coding in modern communication systems. SPb: Science. 2007. 207 p

[3] Fress P, Piaget J. Experimental Psychology (Ed.-Comp.) Moscow: Progress; 1975. pp. 120-125

[4] Feer K. Methods of Modulation and Spreading the Spectrum. Moscow: Radio and Communication; 2000. 518 p

[5] Gnedenko B. Course of the theory of Probability. Moscow: Editorial URSS; 2007. 448 p

[6] Goncharov I, Demyanenko N, Khachumov A, Nozdrachev S. Analysis of the possibilities and systematization of technical means characterizing the construction of a channel for information and psychological impact. In: Proceedings of the Russian Scientific and Technical Conference. Voronezh: Publishing house VSU; 2009. p. 168-174

[7] Goncharov I, Demyanenko N, Mishina Y. Formalization of the Process of Information-psychological Influence. Vestnik VGU, System Analysis and Information Technologies. Voronezh: Publishing house VSU; 2012;**2**(36):41

[8] Goncharov I, Demyanenko N, Mishina Y. Possibility of modeling the process of information-psychological impact with the help of neural networks. In: XIII International Scientific-methodical Conference "Informatics: Problems, Methodology, Technologies". Voronezh: Publishing house VSU; 2013

[9] Goncharov I, Gerasimenko V, Vorobyova E, Dmitriev Y. Technical Means of Ensuring Information Security. Voronezh: VSTU; 2004

[10] Goncharov I, Mishina Y. Description of the approach to the representation of the states of objects and subjects of the process of information-psychological impact with the help of

wavelet transform. In: International Scientific-practical Conference “Technique and safety of the objects of the penal system-2013”. Voronezh Institute of the Federal Penitentiary Service of Russia; Voronezh. 2013

[11] Goncharov I, Parinov P. Models of Information-psychological Impact. Vestnik VSU System Analysis and Information Technologies. 2017;**3**(65):71c

[12] Goncharov N. Justification of the approach to assessing the security of information in modern wireless networks. In: Sirota A, Goncharov I. Scientific Publication “Fundamental Problems of System Security” Materials of the III School-seminar of Young Scientists, May 26–28, 2016, Part 1 – Yelets: YSU them. I.A. Bunin. 2016. p. 87-100

[13] IEEE Standard Association. Available from: http://odysseus.ieee.org/

[14] ISO/IEC 27002 Information technology — Security techniques —Code of practice for information security management. Available from: http://www.iso27001security.com/html/27002.html

[15] Korolev A. Codes and Devices of Noisome Encoding. Minsk. Mn. 2002. 286 p

[16] Kudinov A, Chusova E. The research of loss stability of the level of psychical reaction of a human with the power of informational influence on him, bulletin of PFUR. Series mathematics. Information Sciences Physics. 2014;**2**:259-262

[17] Lieberman Y, Lieberman M. Experience of investigating the effectiveness of memoarherapy. Ekaterinburg: USPU; 2013. p. 192-200

[18] Lieberman Y, Matveva T. Training as a process of managing the level of knowledge and skills. Ekaterinburg: Economics of Education; 2006. p. 192-199

[19] Lieberman Y, Metelkov V. Mathematical model of the level of a person's psychic reaction and its investigation. Successes of Modern Natural Science. 2004. p. 10-14

[20] Naenko N, Ovchinnikova O. Problems of Engineering Psychology. Moscow: Nauka; 1969

[21] National Vulnerability Database [Electronic resource]. National Institute of Standards and Technology. Available from: http://nvd.nist.gov

[22] Prokis J. Digital Communication (trans. with English). Moscow: Radio and Communication; 2000

[23] Roshan P, Liery D. Fundamentals of Building Wireless LANs of the Standard 802.11 (Per. with English) Moscow: Williams Publishing House; 2004

[24] Sklyar B. Digital Communication: Theoretical Foundations and Practical Applications. Moscow: Vilams; 2016. 1104 p

[25] Standards for Security Categorization of Federal Information and Information Systems. Available from: https://www.nist.gov/publications/standards-security-categorization-federal-information-and-information-systems

[26] Venttsel E, Ovcharov L. Chapter 10: Markov processes: Streams of events: Theory of queuing. In: Theory of Probability. Moscow: "Science" (The Main Publishing House of the Physics and Mathematics Literature); 1969. 368 p

[27] Vyalykh A. Dynamics of vulnerabilities in modern secure information systems. In: Vyalykh A, Flacky S. Bulletin of the Voronezh State University. Series: System Analysis and Information Technology. Voronezh: Publishing house VSU; 2011;**2**:59-63

[28] Vyalykh A. Assessment of the vulnerability of modern information systems. In: Vyalykh A, Vyalykh S. Informatics: Problems, Methodology, Technologies: Mater. XI International. Sci. Method. Conf., Voronezh, February 10–11, 2011. Vol. T.1. Voronezh: CPI VSU; 2011. pp. 168-172

[29] Yerkes RM, Dodson JD. The relationship of strength of stimulus to rapidity of habit-formation. Journal of Comparative Neurology and Psychology. 2014;**18**(5). Available from: http://onlinelibrary.wiley.com/doi/10.1002/cne.920180503/pdf