Adaptation of a Risk-Based Approach to the Tasks of Building and Functioning of Information Security Systems

Oleksandr Arkhypov[1], Yevheniia Arkhypova[1] and Jan Krejčí[2]

[1]National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", 37, Prosp. Peremohy, Kyiv, 03056, Ukraine
[2]Jan Evangelisty Purkynė University, Ceske mladeze, 8, Usti nad Labem, 40096, Czech Republic

Abstract

The main aspects and prospects of using the adaptation principle (primarily risk-oriented adaptation) for the construction and functioning of the information security system (ISS) are considered. It is proposed to implement a risk-oriented approach, taking into account the properties and characteristics of the protected information, its social significance and importance, which implies building an objective model of the attacker, assessing his potential and the degree of interest in the successful implementation of the attack. The features and possibilities of practical application of pragmatic aspects of protection are investigated. The content of the basic concepts of adaptive management of the ISS at various stages of information technology development is analyzed. A retrospective of the development of destructive actions in cyberspace and a retrospective of defense paradigms ("digital fortress", alleged violation and proactive defense) are shown. As an alternative to the currently popular methods of building an ISS, it is proposed to use an adaptive approach, the essence of which is to use information about the characteristics and behavior of both parties to the conflict when creating and managing ISS. Mathematical models of reflexive risks are presented, the structure and set of which are determined by the selected typical scenarios for the development of the "attack / defense" situation. Analysis and research of models provides evaluative information that allows to ensure effective and rational investment in the organization's information security, balancing the financial and economic capabilities of the organization with its requirements and capabilities in the field of information security.

Keywords

Adaptation, prioritization, threat, risk-based approach, reflexive model, defense paradigm.

1. Introduction

Today the security of information resources and information and communication systems in which they circulate is one of the main components of the normal functioning of any organization. Consequently, measures to ensure the security of information resources, the creation and support of the information security systems operability are an integral attribute of the activities of various organizations, regardless of their size, types and forms of ownership.

CITRisk'2021: 2nd International Workshop on Computational & Information Technologies for Risk-Informed Systems, September 16–17, 2021, Kherson, Ukraine
EMAIL: sonet0515@mail.com (O.Arkhypov); evgar55@gmail.com (Ye.Arkhypova); jan.krejci@ujep.cz (J.Krejčí)
ORCID: 0000-0001-6832-2223 (O.Arkhypov); 0000-0002-1640-1488 (Ye.Arkhypova); 0000-0003-4365-5413 (J.Krejčí)

We can state the fact that the mutual competition of two oppositely directed processes – the constant development and emergence of new strategies and tactics for implementing information attacks on the one hand, and the improvement of information protection systems that resist these attacks on the other hand – is an absolutely natural social phenomenon. That is why practically any ideology of building an information security system (ISS) contains elements of an adaptive approach, the essence of which is the organization of such a set of protective services (functions) of ISS, which is able to prevent the implementation of threats in relation to the protected information. A successful information security system must guarantee the completeness and timeliness of adaptation of the protection functionality to possible external and internal threats. Therefore, the establishment of a set (list) of these threats is an urgent task, the comprehension and solution of which has given rise to several options for adapting information security systems.

2. Related works

Chronologically, the first variant of the adaptation of information security systems, corresponding to the early stage of development of information technologies used in information and communication systems (ICS), can be called ***natural adaptation*** [1]. The stage of natural adaptation is characterized by the fact that technologies that had a sufficiently high level of typification and standardization of the proposed solutions, implemented by means of unified software and hardware ICS, were used to obtain, transport and process information. Analysis of incidents recorded during the exploitation of such unified ICS made it possible to identify characteristic vulnerabilities in their components, which made it possible to organize and carry out typical attacks that damage the information circulating in ICS. The study and generalization of methods for preventing such attacks led to the construction of stable templates for typical solutions to protection problems and the formation of a corresponding set of functional security requirements – a protection profile.

The implementation of the provisions of natural adaptation during the creation of an information security system ensures the selection of an adequate protection profile, for which it is necessary to comply with the principle of complete overlapping of threats. These provisions formed the basis for the development of the first standard in the field of information security – the so-called “Orange Book” [2], which was the progenitor of a numerous series of national and international standards, and the very idea of compiling a complete list of ISS vulnerabilities was actually erected as a norm in the ISO/IEC Standard 15408.

Unfortunately, with the current level of information technology development, when building an information security system, it is clearly not enough to take into account only retrospectively identified threats. The constantly increasing intensification of development rates, volumes and areas of application of information technologies is expectedly accompanied by a sharp growth in ICS vulnerabilities and, consequently, an increase in the number of potential attacks that exploit these vulnerabilities. The desire to compile the most complete list of ICS vulnerabilities requires a very detailed, lengthy and laborious analysis, based on the results of which a constant expansion of the protection functionality is carried out.

This version of the ISS adaptation could be called ***asymptotic adaptation*** [1], since such a protection system presupposes a complete overlap of threats, which requires an exorbitant investment in its development and modernization. In reality, when constructing an information security system, the possibility of taking into account the unrestrictedly increasing volume of information about the vulnerabilities and threats of ICS is actually excluded [3, 4], which allows

speak only of a hypothetical implementation of the asymptotic adaptation of the information system.

The appropriate way out of this situation is to reduce the set of "all possible" threats to a group of so-called actual threats, which are the most dangerous both for the information resources of the organization and for the assets of the organization as a whole. The identification of actual threats is based on the results of the procedure of threats prioritization [5] – threats ranking (ordering) according to a certain indicator or system of indicators. There are various ways of prioritization: they are mainly based on expert assessments [3, 5-8], but some researchers suggest other ways, for example, risks prioritization by software tools, in particular based on the Common Vulnerability Scoring System [9, 10] or prioritization of vulnerabilities of ISS based on their association-likelihood with exploits [11]. The ISO/IEC standards 27XX series, in particular in the ISO / IEC 2705 standard, for threats prioritization recommended using risks of information security. Let's call the ***risk-based*** or ***risk-oriented adaptation*** the process of forming the structure and composition of the information security system, based on the identification of a group of urgent threats, which are the main source of the most significant information risks for the organization.

The ***aim*** of this work is to consider the main aspects and prospects of using the adaptation principle (and, first of all, risk-oriented adaptation) for the construction and functioning of the information security system. The proposed adaptation of the risk-oriented approach is carried out taking into account the properties and characteristics of the protected information, its social significance and importance and involves building an objective model of the attacker, assessing his potential and the degree of interest in the successful implementation of the attack.

3. Risk-based adaptation

Risk-based adaptation involves the successive implementation of two tasks:

- identification of threats to information security that are relevant for this particular organization, taking into account its goals and the functioning specifics;
- building an information security system based on the study and analysis of properties of actual threats and sources of their origin.

The content of the first task, i.e. the selection of a group of actual threats (sometimes is used semantically similar term “significant” threats), consists in ranking (ordering) information threats according to the degree of danger they pose to the organization, which is implemented through analysis and comparison of threats to each other according to the severity of their specific properties, called dangerous factors [6]. Exactly this procedure for comparing and ranking threats is called threat prioritization [5] or less often – “filtering” threats [12].

Depending on the depth and detailing of the analysis performed, a different number of factors can be used to describe the threat, i.e. conducting a comparative analysis of threats to compare and rank their degree of danger is based on the vector characteristics of threats, and the dimension of the vectors for different threats may be different, which complicates prioritization. For example, in [12], in order to classify threats as relevant, the following factors are supposed to be analyzed:

- the presence of vulnerabilities in the ICS, allowing the possibility of threat implementation;

- the likelihood of successful implementation of attacks that exploit the identified vulnerabilities;
- the amount of losses (damage) inflicted on the organization in case of successful implementation of the threat.

When quantitatively setting the values of losses and probabilities, following the above-mentioned recommendations of the ISO/IEC standards 27XX series on intensively involving a risk-based approach in information security management practice, it is quite simple, by calculating the risks of attacks, to reduce the vector description to a scalar one, and then, by aggregating the risks of attacks into risks of threats, to order the threats in descending order of their risk magnitude.

Researchers and practitioners offer different ways of prioritization: by vulnerabilities, risks, threats, but in fact all of them are variations of one of the most general prioritization schemes. The starting point of this scheme is to compile the most complete “starting” list of ICS vulnerabilities. The exploitation of a single vulnerability or their set (“chain of vulnerabilities”) allows you to implement an attack, the effectiveness of which is characterized by the level of private risk arising from the violation of the normal mode of operation of the organization. The criterion of insufficient effectiveness of the attack is a negligibly small level of private risk generated by it, which is the basis for excluding the vulnerability that determines the possibility of this attack from the "starting" list of vulnerabilities. At the same time, a list of actual threats is formed, which includes threats implemented by one effective attack or a combination of them, provided that the integrated (generalized) risk of the analyzed threat was above a certain minimum threshold level.

Let's consider in more detail certain aspects of prioritization using an illustrative example. Suppose that among the vulnerabilities discovered during the ICS survey, a group of vulnerabilities $\{V = \{v_j\}\}$, $j = \overline{1,k}$ was identified, any of which allows an effective attack, the purpose of which is to implement the threat t. The danger of an arbitrary attack α_j is characterized by its particular risk

$$\rho_j = p_{aj} q_{aj}, \quad (1)$$

where p_{aj} is the probability of successful implementation of the attack, q_{aj} is the losses incurred by the organization. If the attacks are independent and incompatible, the danger of threat t as a whole is characterized by an integral risk R_t, calculated for the full group of events, including k dangerous events (set of attacks $A = \{\alpha_j\}$, $j = \overline{1,k}$,) and one (k+1)-th event, which corresponds to the ICS safe operation mode (absence of any attacks / threats) with parameters: $q_{\alpha,\, k+1} = 0$,. $p_{\alpha,\, k+1} = 1 - (p_{\alpha 1} + \cdots + p_{\alpha k})$. In this situation, the calculation of the integral risk R_t is carried out using the formula for the total risk R_Σ [4, 6] aggregating the risks of individual attacks:

$$R_t = R_\Sigma = \sum_{j=1}^{k} p_j = \sum_{j=1}^{k} p_{aj} q_{aj}\,, \quad (2)$$

In the general case, when calculating the integral risk R, a methodological problem arises, which is typical for the case when the threat is realized by carrying out several so-called cooperative attacks (in [4] the term simultaneous attacks is used). The implementation of cooperative attacks leads to an increase in the likelihood of the analyzed threat and, as a consequence, to an increase in the level of integral risk introduced by it, the calculation of which in this case encounters certain difficulties. For a more adequate understanding of the problem, we will slightly change the wording of the above example: we will cancel the requirement of

incompatibility of attacks and assume that the successful completion of any of the attacks leads to the same losses q. If in this case to calculate the integral risk R_t of a threat t we apply the formula for the total risk, we get:

$$R = R_{\Sigma} = \sum_{j=1}^{k} p_j = \sum_{j=1}^{k} p_{aj} q = q \sum_{j=1}^{k} p_{aj} \quad (3)$$

On the other hand, if the probability p_t of the threat t realization is known, the risk of threat t is calculated using the formula $R = qp_t$. Comparing this formula with expression (3), we obtain equality:

$$p_t = \sum_{j=1}^{k} p_{aj}, \quad (4)$$

moreover in this case, for the probability p_t, like any other probability, the requirement $0 \leq p_t \leq 1$ must be fulfilled. However, the right inequality in this requirement for attacks, the probabilities of which satisfy the condition $1/k < p_{aj} \leq 1, j = \overline{1,k}$ obviously does not hold:

$$p_t = \sum_{j=1}^{k} p_{aj} > 1 \quad (5)$$

Therefore, in the most general case, formula (3) is not correct, and the risk value R calculated from it may turn out to be overestimated. The reason for this situation is the inapplicability of the total risk formula for calculating the integral risk of a threat in the event of cooperative attacks. The methodically correct method for calculating the assessment of integral risk in this situation is described in [6], its development, features of practical application – in [2].

To get acquainted with the essence of the proposed methodology, let us consider a scenario in which the threat t is supposed to be implemented by the cooparative (simultaneous) implementation of two independent attacks α_1, α_2, the probability of successful completion of which is, respectively, $p_{\alpha 1}, p_{\alpha 2}$. To calculate the integral risk R_t of a threat t, we form a complete group, represented by the tuple $A_4 = < \alpha_1\alpha_2, \alpha_1\overline{\alpha_2}, \overline{\alpha_1}\alpha_2, \overline{\alpha_1}\,\overline{\alpha_2} >$, of four pairwise incompatible complex bipartite events, where $\overline{\alpha_j}$, $j = 1,2$ is the event opposite to the event α_j, therefore, for the probability $\overline{\alpha_j}$, the following relation is valid: $P(\overline{\alpha_j}) = (1 - p_{\alpha j})$. Combining two joint events – independent attacks α_1, α_2, is equivalent to combining the first three inconsistent elements of a tuple A_4 – complex binary events $\alpha_1\alpha_2, \alpha_1\overline{\alpha_2}, \overline{\alpha_1}\alpha_2, \overline{\alpha_1}\,\overline{\alpha_2}$. Consequently, the integral risk caused by the implementation of two cooperative independent attacks α_1, α_2 is equal to the total risk from the implementation of three incompatible complex independent attacks (events) $\alpha_1\alpha_2, \alpha_1\overline{\alpha_2}, \overline{\alpha_1}\alpha_2, \overline{\alpha_1}\,\overline{\alpha_2}$. We calculate the probabilities of these incompatible complex attacks: $p_{12} = p_{a1}p_{a2}$, $p_{10} = p_{a1}(1 - p_{a2})$, $p_{02} = (1 - p_{a1})p_{a2}$, $p_{00} = (1 - p_{a1})(1 - p_{a2})$ and estimate the corresponding values of losses, for example, we assume that $q_{12} = q_{10} = q_{02} = q$, $q_{00} = 0$. As a result, we obtain quite correct ratios for the threat t: the probability of the threat realization, represented in terms of the probabilities of attacks, is

$$p_t = p_{12} + p_{10} + p_{02} = 1 - p_{00} = p_{a1} + p_{a2} - p_{a1}p_{a2}, \quad (6)$$

and, accordingly, the risk of a threat is

$$R = (p_{12} + p_{10} + p_{02})q = qp_t \quad (7)$$

In a real situation, the losses q_1, q_2 arising from the implementation of each of the attacks may not coincide with each other, and therefore the losses caused by the implementation of incompatible complex attacks will differ: $q_{12} \neq q_{10} \neq q_{02} \neq q_{00} \neq q$, $q_{00} = 0$. Then the value of the integral risk R_t of the threat t is calculated using the general formula for the total risk

$$R_t = p_{12}q_{12} + p_{10}q_{10} + p_{02}q_{02}, \quad (8)$$

and then we find the value of integral (cumulative) losses due to the implementation of the threat t:

$$q = R_t/p_t. \quad (9)$$

After calculating the integral risk R_t, calculating the relative risks of attacks: $p_{a1}q_1/R_t$, $p_{a2}q_2/R_t$ and, comparing these values with each other or comparing them with a certain threshold value δ, we make a decision about the effectiveness (efficiency) of each of the attacks. In particular, a low level of relative risk is a criterion for insufficient effectiveness of an attack and serves as the basis for excluding the vulnerability that determines the possibility of this attack from the "starting" list of ICS vulnerabilities.

In general, the number of cooperative attacks undertaken to implement a threat t may be more than two. Unfortunately, as the number of n=2, 3, 4, ..., increases, the number of ... pairwise incompatible complex attacks that form the complete group of n- events represented by the tuple A_N, the total risk of which corresponds to the value of the sought integral threat risk, increases at an outstripping tempo $(N = 2^n = 4, 8, 16, \dots)$. As you can see, the above-described methodology for calculating and analyzing risks requires rather cumbersome calculations involving quantitative information on the probabilistic parameters of attacks and the magnitude of the damage they cause. But if the formal aspects of transforming probabilistic data are regulated by the proposed methodology, information of an economic nature is mainly set by an expert, which affects the accuracy and objectivity of the final results. Apparently, taking into account all this, in the guidance documents of various levels (standards; industry, departmental, corporate manuals, recommendations, etc.), the emphasis is placed on the presentation of methods and provisions which are working with data in a qualitative form of presentation.

The prioritization schemes considered above, based on the calculation and comparative analysis of the effectiveness of attacks, which became possible due to the existence of a number of ICS vulnerabilities, actually represent the prioritization of vulnerabilities. Identification of actual threats is also found on similar prioritization schemes based on the comparison of losses incurred by the attacked organization as a result of the implementation of a particular threat. The result of the prioritization of threats is the selection of a set of actual threats $T_\alpha = \{t_i\}$, $i = \overline{1, m}$ the generalized characteristic of which is ***the aggregated (generalized) informational risk of an organization***, found by combining (aggregating) individual integral risks of actual threats in one general risk indicator. In some cases, the aggregation procedure can be quite simple. For example, given the independence and incompatibility of the actual threats, as well as the independence of the consequences resulting from their implementation, the aggregated (generalized) integral risk of the organization will correspond to the total risk

$$R = \sum_{i=1}^{n} R_{ti} \quad (10)$$

where R_{ti}, $i = \overline{1, n}$ is the integral risk of each individual threat from the selected group of actual ones. Further, in the same way as when assessing the effectiveness of attacks, the relative risks of individual threats are calculated: $R_{t1}/R, \dots, R_{ti}/R, \dots, R_{tm}/R$ and after comparing these values with each other or comparing them with a certain threshold value Δ, a decision is made about the relevance (significance) of some threat. In particular, the excess by the level of relative risk of threshold Δ is the basis for recognizing the relevance of the corresponding threat.

Unfortunately, for organizations with a rather complex structure, having a significant amount of information resources (IR) and intensively using complex information technologies in their work, the calculation of the aggregated integral risk of an organization R under the conditions of

the possible impact of several threats, allowing joint implementation with the manifestation of interrelated and interdependent consequences, is a very difficult problem, the solution of which is generally absent [6].

The need to solve this problem has stimulated attempts to apply a more globalized approach to considering organizations and their aggregated integral risks R, within which the technological aspects of risk assessment, and primarily the most cumbersome and labor-intensive detailed analysis of ICS threats and vulnerabilities, are practically not used. Instead, focused attention was paid to the study and modeling of conflict situations that arise when a threat t to an information resource I is realized, in particular, the impact on the conflict scenarios of the competence characteristics of its participants, their resource provision, formalization of the dependence of the business of organizations and the total value of their main assets on the level of security and the state of the corresponding information resources.

4. Building an information security system with targeted adaptation to the potentials of the attacking and defending sides

Let us consider in more detail the conflict situation (hereinafter referred to as the "attack / defense" situation), which develops in the event of a possible implementation by the attacker of a threat t regarding the information resource I of a certain organization [3, 13] (the conflict itself will arise with the beginning of active actions). By an attacker initiating a conflict, we mean any entity (hacker, malicious code, internal attacker, etc.) whose malicious actions are aimed at information circulating in the organization's ICS. The successful implementation of the attack will obviously affect the state and value of the assets of the organization (the defending party).

Features of the development of the conflict, its results depend primarily on the ratio of the potentials of the parties to the conflict. The ***potential of the attacking side*** is usually understood as a complex of the following factors: the competence and level of motivation of the attacker (in the case of an anthropogenic nature of the attack), resource support (including financial and economic), contributing to the successful implementation of attacking actions. The possibility of taking these factors into account is considered in [3], where, depending on the presence and severity of these factors, models of typical scenarios of the attacker's behavior are verbally described for a set of typical roles that form a specific role structure (classification):

1. ***Script kiddies*** - as a rule, a loner with little training, knowledge and experience, uses scripts or programs developed by others for an attack, does not understand the mechanism of their action, incapable of creativity, independent effective attack solutions, with rather modest resource capabilities. Usually he is not worried about political or financial considerations, more precisely, financial interest is not the only determining motivation for his actions, since there is usually no idea of the market value of the attacked resource. Most often, the goal of a script kiddie is to impress his surroundings, to gain authority among fellow representatives of his computer subculture, the desire to create chaos, refusal or disruption of services, and finally, just "sports interest" [3]. According to A. Lukatsky [14], script kiddies account for up to 95% of the total number of cybercriminals attacking information and computer systems, i.e. this is the most common type of intruder, the need to protect against which is a primary task when building an information security system.

   It should be noted that various malicious codes (viruses, worms, etc.) can be called a script kiddie attacks, provided that its impact can no longer be qualified as a zero-day attack.

2. ***Self-employed professional***, working alone or as part of a group of professionals, with the necessary knowledge, skills and sufficient experience, well versed in attack technology, with a deep understanding of methods of hacking security systems, for whom hacking is the main activity of an obvious commercial nature, the purpose of which are financial and economic benefits.
3. ***Professional executor*** – a hacker, according to his objective characteristics and capabilities, corresponding to those listed in clause 2, but performing tasks in the interests of law enforcement agencies or special services as a hired executor, acting within the framework of certain mutual contractual relations.
4. ***Hacktivist*** – an ideological hacker ("cyber activist") who uses cyberspace to promote political or social ideas (tasks), organizes actions of civil "electronic" disobedience in cyberspace, trying to draw the attention of the authorities and the public (sometimes in a rather harsh form) to some issues and problems of modern society through the synthesis of social activity and hacking.

Note that for the first three roles in this classification, the main differentiating feature is the level of competence of the attacking side (i.e., the presence of knowledge, skills and practical experience), which is intensively growing in the direction of a kiddie script, a self-employed professional, a professional executor. The basic characteristic of a hacktivist, which distinguishes him from the three previous roles, is that he has certain ideological and moral-ethical attitudes.

It is obvious that the success of the actions of the attacking side, as well as the final scenario of the development and end of the conflict, largely depend on the potential of the defense. The latter is mainly determined by the volume of investments in the information security system, the level s of information maturity ($s \leq 85$, [3]) of the defending party, as well as the integral characteristic of the importance of the protected information resources, which is often determined by the cost or value of the organization's information resources. Further, as this integral characteristic, we will use q – the total (maximum) losses of the defending side in case of successful completion of the attacking actions directed against it.

Each specified role has its own model scenario for the behavior of the attacker. In work [3], mathematical models of aggregated integral risks $R_{(c)}$ are presented, which determine the possible losses of the defending party in the event of a particular role scenario. These risk models reflect the peculiarities of each of the typical roles introduced above, that's why they were called ***reflexive risk models*** (from the Latin *reflexus* – to bend back, turn away). In addition, the models of reflexive risks reflect the difference in the "attack / defense" situations arising from variations in the parameters characterizing the attack and defense potentials, with the same volume of investments in the information security system. In fact, the introduction of reflexive risks makes it possible to implement in a very wide range targeted adaptation of the risk-based approach when it used to analyze specific situations "attack / defense".

Below are some typical reflexive risk models.

4.1. The reflexive risk model for the script kiddie

The reflexive risk model for the first typical role - the script kiddie - makes it possible to assess the aggregated integral risk of an organization in the most "sparing" conditions of its functioning, in the absence of any targeted attacks specially designed against it. The model is given by the formula [3]:

$$\mathrm{R(s,c)} = \mathrm{P_t P_v q} = \mathrm{P_t}\frac{\mathrm{q}}{\mathrm{q+sc}}\mathrm{q}, \tag{11}$$

where P_t is the probability of activation at a given time and place of a threat t to the organization's information resources (an analogue of statistical assessments determined by The National Institute of Standards and Technology, USA); P_v is the probability of successful implementation of an activated threat. In the absence of information about the quantitative value P_t, due to the widespread threat from the script kiddie, as a first approximation, we can assume $P_t = 1$, i.e. the script kiddie is ready to attack anyone, anytime, anywhere, as soon as it becomes possible to perform attacking actions. Purposefully choosing the target of an attack, deliberately planning and developing its scenario in advance, is not for a script kiddie. The nature of the script kiddies actions is well illustrated by the characteristic of their behavior given by W. Stallings [15]: “a dull desire to" knock on closed doors "for an infinitely long time, checking all system vulnerabilities”. This quote to some extent contains an explanation to the formula immediately following from expression (11)

$$\mathrm{P_v} = \frac{\mathrm{q}}{\mathrm{q+sc}}, \tag{12}$$

according to which the probability P_v depends only on the measures to ensure the security of information taken by the defending party, which is consistent with the mentioned feature of the script kiddy behavior, which consists in the absence of novelty in the attacking actions taken by them. In such a situation, the information security system, which implements the principle of complete overlapping of “old” threats and their obvious modifications, is quite reliable. The degree of protection of an organization increases with an increase in the volume of investments c, provided they are used correctly, i.e. with growth s. Analysis of reflexive risk (11), its comparison with the size of investments c in the information security system allows to obtain a formula for determining the effective volume of investments [13]:

$$c_{\mathrm{eff}}(s) = \underset{c\in C}{\mathrm{argmax}}(\mathrm{R}(s,c) - R(s,0) - c) = \underset{c\in C}{\mathrm{argmin}}(\mathrm{R(s,c)} + \mathrm{c}) = \frac{q}{s}(\sqrt{P_t s} - 1), \tag{13}$$

where C is a set of values c representing “reasonable” investments (for which “risk savings” $\Delta_R(s,c) = R(s,c) - R(s,0) > c$), concentrated in a range $0 \le c \le q(s-1)/s$. Within the range of “reasonable” investments, the dependence of the values of the effective volume of investments c_{eff} on the parameter s has a single-extreme character with a maximum equal to $\max[\mathrm{c_{eff}(s)}] = 0{,}25\mathrm{qP_t}$ [3].

If P_t=1, the value of effective investments in the information security system is expected to be the largest, i.e. the value of the maximum investment in the information security system will be $c_{eff\,max} = 0{,}25q$ or 25% of the cost of the resource q, which is the object of protection. However, for productive security solutions (for example, at $s = 60$) in accordance with formula (10), even at P_t=1, the volume of investments in the ISS may turn out to be at the level of 11-13% of the cost of the protected resource, and at the highest level of information culture of the organization's employees, i.e. according to [3], with a value of $s = 85$ – 9,67%. The obtained results are in good agreement with a number of existing empirical estimates of the volume of investments, in particular, with the data given in publications [7, 12], the authors of which focus on the amount of 15-20% of the value of information system assets.

Thus, the results obtained in the course of the study of the reflexive risk model (11) allow in a real situation, knowing the values of the parameters $\mathrm{q, s}$, to find estimates of indicators $\mathrm{c_{eff}}$, $\mathrm{c_{eff\,max}}$, $\mathrm{R(s, c_{eff})}$ and to set the value of an acceptable for a given organization “reasonable” volume of investments in the information security system [3, 6]. Considering this object as a resource constraint, we could proceed to solving the problem of assignment of

allocated investments on a limited set of possible functions and protection mechanisms, forming on them the structure of the information security system from the condition of minimizing the residual risk of the organization, comparing and analyzing quantitative estimates of indicators c_{eff}, q, $c_{eff\,max}$, $R(s, c_{eff})$, $R(s, c)$ for various values parameter c, while balancing the financial and economic capabilities of the organization with its requirements and capabilities in the field of information security.

4.2. The reflexive risk model for the self-employed professional

Reflexive risk model for the second typical role - self-employed professional, given by [3, 13] expression

$$R(s, c) = P_t P_v q = \left(1 - \frac{D}{g}\right) \frac{q}{q + s\,\frac{c^2}{D}}\, q. \tag{14}$$

where g is the value (importance) of the resource for the attacking side, D is its generalized costs of preparing and implementing attacking actions, reduced to the monetary form of representation. The appearance in the risk model of new parameters g and D, characterizing the interests and motives of the attacker's behavior, is due to the adaptation of the risk model to a new typical role, which is characterized by a significant influence of the attacker's capabilities on the outcome of the conflict. In particular, the first factor on the right-hand side of expression (14), which is an estimate of the probability P_t of threat t activation

$$P_t = \frac{g - D}{g} = 1 - \frac{D}{g}, \tag{15}$$

admits the following logical-heuristic interpretation: the higher the net profit $g - D$ received by the attacker in the case of the successful implementation of the threat, the higher the attack motivation. In fact, the probability P_t in formula (15) is the profit related to the value of the resource I, i.e. an indicator of the effectiveness of the alleged attack: the more g, the closer to 1 the probability P_t; with a decrease g, in the case $g \le D$, the conduct of the attack loses its meaning (if the attacker's motivation is limited by the scope of commercial interest). In practice, this means that the likelihood of high-cost attacks being deployed by a purely commercial professional is extremely low. Finally, when $g \gg D$ the probability P_t is practically equal to 1, a so-called “targeted attack” takes place, a characteristic feature of which is the presence of a specific target - an object of attack (organization, department, individual) against which active attacking actions are carried out.

The influence of the attacking side is also manifested in the modification of the structure of the heuristic used to calculate the probability P_v estimate: a multiplier $k = c/D$ is introduced into the denominator of expression (12), which makes it possible to correlate the volumes invested by the sides in defense and attack. As a result, for P_v we obtain a new heuristic used in formula (14) [3, 6]:

$$P_v = \frac{q}{q + skc} = \frac{q}{q + sc^2/D}, \tag{16}$$

The range of reasonable investments corresponding to model (14) is given by inequality [3]:

$$\frac{qP_t}{2}\left(1 - \sqrt{1 - \frac{4D}{sqP_t^2}}\right) \le c \le \frac{qP_t}{2}\left(1 + \sqrt{1 - \frac{4D}{sqP_t^2}}\right). \tag{17}$$

It should be noted the presence of a number of modifications of the model (14), due to the desire to ensure a deeper adaptation of this model of reflexive risk to a particular feature of the "attack / defense" situation. For example, in [6], to estimate the probability P_t of threat t activation, next formula is proposed:

$$P_t = 1 - \frac{D}{\gamma g}, \tag{18}$$

where γ is an additional parameter that takes into account the "individual" characteristics of the attacking side: excitement, adventurism, excessive self-confidence ($\gamma > 1$) or, on the contrary, excessive caution, indecision, self-doubt ($D/g < \gamma < 1$). This problem can be considered in another setting, since commercial interests, the principle of economic expediency and pragmatism do not exhaust the possible motives that the attacking side is guided by in its actions. In particular, a desire for revenge, punishment, asocial and other aspirations, the result of which could be the intention to inflict as much damage on the defending side as possible (financial, political, image, moral, etc.). In this case, the activation probability P_t can be given by the formula

$$P_t = 1 - \frac{D}{q}, \tag{19}$$

according to which the maximization of the probability P_t occurs with an unlimited increase in damage q arising from the implementation of information threats. This situation demonstrates the possibility of transforming the risk model (14) of a self-employed professional (by means of its fragmentary modification, detailing or simplification) into other models corresponding to other scenarios of the attacker's behavior.

4.3. Professional executor

In particular, an example of circumstances in which the principle of economic expediency for the attacking side turns out to be insignificant is the performance of a particularly important task by intelligence officers – professionals trained to carry out attacking actions in cyberspace [3, 13]. In this case, the task of the attacking side (the practical implementation of some threat to the resource I) must be performed in any situation, i.e. with a probability $P_t = 1$, that distinguishes this typical role from the previous one, in which the attacking side in its actions proceeds exclusively from the provisions of economic pragmatism. Due to the special importance of the task at hand, when solving it, usually existing restrictions are removed. In particular, the performer can count on attracting various additional resources to support his actions [3]. This formulation of the question makes it possible to ensure the implementation of extremely high-cost attacks ($D \to \infty$).

The reflexive risk model for this case is simple:

$$R(s, c) = P_v q = \frac{q}{q + s\frac{c^2}{D}}\, q. \tag{20}$$

It is obvious from it that with the removal of resource constraints ($D \to \infty$), the probability $P_v \to 1$, that is, in this situation, if the defending party, creating its own information security system, relies on the principle of reasonable sufficiency, proceeding solely from its own ("internal") understanding of the existence of the final value q of the protected resource I, the successful implementation of the threat by the attacker is practically guaranteed, so $R(s, c) \to q$.

What attacks and threats lead to reflexive risks (14) and (20)? A self-employed professional uses a very wide range of attacks, ranging from massive (DDOS attacks, phishing, ransomware viruses, etc.), social engineering attacks and ending with individual targeted attacks. Professional executor uses all this attacks as well as advanced persistent threat (other common translation options: complex targeted threat [16], complex extended (constant) threat [17], complex, advanced and persistent attack aimed at seizing control over the target infrastructure [7]).

5. The main paradigms of information protection

To clarify the actual role and essence of adaptation in the formation of information security systems, it is advisable to give a retrospective of the development of destructive actions in cyberspace and defense paradigms. As a starting point, let's take the Morris worm attack on the Advanced research projects agency network (ARPANET), which at that time (november 1988), in terms of complexity and its consequences, in particular, the amount of damage, the estimates of which range from $ 98 million to $ 300 million, is quite consistent with the current threats of APT-class. The reaction to it in the field of information security was the creation at The University of California and Carnegie Mellon University a Computer emergency response team (CERT). In the late 1980s and the first half of the 1990s, a significant part of computer security incidents were the results of single targeted attacks organized on a specific order. During this period, the analytical work of CERT experts involved in the collection of information about incidents, their classification and neutralization, contributed to the preservation of a fairly stable and high level of cybersecurity.

However, the attacker, analyzing and comprehending the results of single attacks, began to repeat (replicate) successful solutions. As a result, many attacks became massive, not targeting a specific object, for example, a bank or a specific client. During this period, it turned out to be more profitable for the criminal market to develop and sell not unique, but mass attacking actions. Mass virus attacks, sometimes taking on the character of epidemics, have become especially popular.

In such a situation, defending against massive attacks, the defense side was guided by the ***"digital fortress" paradigm***, the properly organized defense of which excluded the enemy's penetration through the defense perimeter. The success and consistency of protection was based on the results of a retrospective analysis of incidents that occurred earlier on the assumption that the conditions for the functioning of the ICS, the information technologies used in them and the software and hardware tools involved in this process remain unchanged. But when the defense learned how to effectively fight off massive threats, the trend of attacks began to change again: targeted attacks began to be implemented again, but in a higher professional performance. And while the "digital fortress" paradigm remained effective against attacks from the script kiddie, it turned out to be untenable to protect against professional attacks. This became apparent at the end of the first decade of the 21st century, when a number of successful attack actions practically proved the impossibility, within the framework of the requirements of most traditional information security management guidelines, based on the analysis and study of previous incidents and taking into account the properties of retrospectively identified threats, to provide the required level of information security.

This conclusion led to the postulation of a new ***paradigm of assumed breach***, the essence of which is that the defending party must assume that its information system can and will be breached [18]. This paradigm has been perceived in different ways by security professionals, mainly due to differences in the interpretation (understanding) of its content. Some saw the need

to shift the emphasis of protection towards ensuring the continuity of business processes, abandoning effective disaster recovery plans, reducing the damage caused by implementing a set of actions covering a very extensive list of measures, starting with purely technical issues of backup, data mirroring, information recovery and to economic and organizational measures, including the transfer of risks, insurance, etc. However, in most cases, in fact, the essence of the new paradigm consisted in expanding the scope of protective actions, suppressing attacks and eliminating threats both at the perimeter border and after overcoming it: the defense methodology changed, adapting to the current balance of potentials and real capabilities of the parties to the conflict. A characteristic feature of the protection paradigm is the implementation of adaptive information security management by monitoring possible attacks in real time or with a slight delay due to the need for additional information to make an objectively informed decision based on monitoring data. In particular, the urgent need to detect and analyze new, emerging threats (zero-day threats) was realized by searching for and isolating behavioral anomalies in the ICS functioning environments, using sandboxes, traps, and other possible means and methods of detecting attacks. Thus, for this paradigm, the transition from the use of a methodology based on the principles of monitoring a certain set of static indicators that retain relative stability during the implementation of massive (replicated, repeated) attacks, to a dynamic one is obvious.

But the methods mentioned above, which more or less justify themselves when protecting against targeted attacks, quickly became quite understandable for the authors of modern attacking technologies, which ultimately sharply worsened the situation with protection against complex attacks that are being implemented today in cyberspace, in particular, against advanced persistent threats.

A paradigm for the development of ISS, based on persistently declared approaches and principles of ***proactive protection*** [8, 19-22] seems to be promising for this case. Unfortunately, there is still no single generally accepted interpretation of this term. Recently, proactive protection is most often understood as actions of a proactive nature taken by the defending party in order to detect and prevent attacks before they lead to any negative consequences. At the same time, as noted above, to build a truly robust security system, it is not enough to ensure the security of the network perimeter, it is also necessary to ensure control of critical data by monitoring any activity in the information system and tracking all system messages for suspicious changes.

According to experts [17, 14], many complex cyberattacks are undetected, and those that have been detected are not made public due to reputational risks, and therefore it is not possible to offer any typical method for identifying these attacks even for organizations that investigate incidents and analyze the actions of hacker groups. The approaches used to detect attacks are often based on the use of dynamic analysis of a set of anomalies in the states of various ICS elements. If these anomalies can be linked together in a single cause-and-effect chain, proposing a plausible scenario for the development of a complex attack, there is a real possibility of predicting its negative consequences with the subsequent application of the classical methodology of a risk-based approach to make a decision on taking adequate protective measures. Most of the results obtained as part of such a procedure for identifying and suppressing ATP-threats are predominantly analytical in nature and are formed in the Security Operations Center (SOC) by a team consisting mainly of security analysts, whose tasks include detecting and analyzing incidents of cyber security, prompt response and prevention of its occurrence, reporting.

It should be noted that there are other interpretations of the concept of "proactive defense", for example [19]:

- attacking actions taken against an enemy preparing an attack;
- a preemptive attack based on evidence that an enemy attack is inevitable;
- actions taken directly against the enemy at the preventive stage of his attack.

Obviously, when accepting any of the above formulations of the concept of “proactive protection”, the direct launch of the procedure (mechanism) for its implementation should be preceded by a large amount of analytical work performed in the SOC. Thus, again, like thirty-three years ago (during the organization and formation of CERT), the main emphasis in ensuring security is shifted towards expert analysts, whose activities, ideally, should guarantee the adaptation of information security mechanisms to reflect any arbitrarily complex, constantly changing threats. The difference is that the SOC deals with internal incidents or incidents aimed at the internal information assets of the organization, while the CERT serves a higher level of threat analysis, its scope is department, industry and beyond.

The emergence of the SOC indicates that professional attacks, in particular sophisticated ATP-attacks, are becoming widespread. This is confirmed by the published statistics. Thus, according to the classification of A. Lukatsky in 2003 [14], all attacks were divided into “known” and “unknown” in a ratio of 95% to 5%. In 2015, specialists of Kaspersky Anti Targeted Attack Platform [16], in addition to "known" and "unknown", single out "complex" attacks (70%, 29% and 1%), while after 2 years their classification based on the analysis attacks in 2016 is changing significantly: they distinguish [7]: “common threat” – 90%, “complex attacks” – 9%, “unique attacks” – 1%. As you can see, the division of attacks into “known” and “unknown” has lost its relevance, and the number of “complex attacks” has increased 9 times over two years.

At first glance, the above data simply indicate an increase in the number and qualifications of attackers. However, the real situation is much more complicated. In the field of cyber-attacks, a full-fledged service market has emerged that allows newcomers to cybercrime not to waste time and effort on learning all the intricacies of the “craft” and developing their own product, but simply buy a ready-made service or product from more experienced hackers. Professional cybercriminals and criminal organizations develop cyberattack tools and end-to-end services to sell to other, usually less experienced, criminals. The corresponding term – Crimeware-as-a-Service (CaaS) – has appeared and is gaining popularity. Crimeware-as-a-Service refers to the practice in the cybercriminal ecosystem to provide products and services to other cybercriminals [23].

CaaS provides an attacker with a sufficiently developed toolkit (for example, buying a ready-to-distribute version of the ransomware on the Darknet market, which is enough to configure and release it on the network, or a new version of a Trojan with a well-thought-out distribution strategy). The use of the outsourcing model in organizing cyberattacks is becoming relevant, when hackers carry out cyberattacks as a commercial service. For example, on the Darknet you can find relatively inexpensive offers for organizing “commercial” DDoS attacks, the cost of which depends on the power and duration of the attack, as well as the parameters of the server on which the victim site is located), renting botnets, selling or renting software codes of malicious software, including encryption programs [24-26]. So, in 2015, the Ransomware-as-a-service scheme appeared, through which any completely ordinary user can order a very advanced cyberattack involving a ransom demand [26].

An analysis of numerous reports, reviews, analytical articles of recent years shows that the above-mentioned changes in the field of cyber-attacks have stimulated the process of intensive blurring of the competence boundaries of the first three levels of role classification. In particular, for the most energetic and trained novice hackers in the current qualitatively new situation, a sharp increase in the level of practical skills, evolving to complex techniques, became possible, which allowed them to quickly, practically bypassing the stage of "script kiddie", declare themselves as professionals. The latter, in turn, contributed to the emergence and rapid build-up of a powerful transitional reserve, whose representatives "diffuse" higher into the layer of professional performers.

In general, attackers are becoming more organized and rational in terms of the costs of preparing and conducting attacks, minimizing their expense, which contributes to the growth of the profitability of attacks and, as a consequence, an inevitable increase in their total number and variety. Therefore, for all the pretentiousness of the proactive defense paradigm, the idea of preventing all incidents before they occur is unjustifiably expensive and, therefore, untenable from the point of view of the resources involved for its implementation. There are many incidents that are cheaper to eliminate once they occur than to prevent in a proactive paradigm. For example, now the increased activity of ransomware confronts business with a choice: either to invest heavily in security, trying in principle to exclude the possibility of a ransomware attack, or to limit itself only to reactive protective measures characteristic of the paradigm of imminent hacking of the security perimeter. Thus, the implementation of the paradigm of proactive protection in its practical implementation inevitably faces the need for a reasonable balancing of proactive and reactive mechanisms for ensuring information security. The basic information that allows this balancing to be carried out, while remaining within the framework of economically acceptable investment decisions, are estimates of the maximum investment volume $c_{eff\ max}$.

6. Conclusions

The development of the situation in the field of information security in a number of cases is advisable to represent in the form of a model of a bilateral conflict "attack / defense", where the defense side is the owner of the information, the purpose of which is to ensure the security of information belonging to him from the encroachments of the second party to the conflict - the attack side, which in reality can represent a set of attackers who act independently or in cooperation with each other. The conflict is of a process nature, the attacking side is active, updating and improving its methods and tools, thereby contributing to the efficiency and profitability of its actions. As a result, the defending party is also forced to constantly modify its protection system, although the performance of protective functions is not its direct task and is of a supporting nature, only contributing to the successful implementation of the main activities of the organization-owner of the information. Therefore, for the side of the defense, the task of minimizing investments in information security is very important while maintaining acceptable indicators of stability and safety of its main activity.

If during the construction of the first information security systems the norm was to overlap all directions of attack implementation, then with the growth of their number, only relevant (significant) from the point of view of the defending side of the attack, highlighted (prioritized) by the use of a risk-oriented approach, were blocked. This, to some extent, made it possible to reconcile security requirements with the need to allocate the minimum required investment in information security. However, the increasing complexity of the methods of implementing threats has led to the need to take into account and analyze the relevance of all possible attacks,

leading to a rapid increase in their total number, which ultimately made a full-fledged and non-subjective application of the risk-based approach almost impossible. The emerging problem was resolved by a change in the defense paradigm. The new paradigm has simplified the adaptation of methods and defense mechanisms to targeted rationally planned attacks, while simultaneously becoming a new incentive for the attacking side to develop even more complex unique targeted attacks of the ATP-class. In turn, this again prompted the introduction of new changes in the protection methodology, the formation of the next update of its paradigm. In fact, there is a continuous process of mutual development of both conflicting parties, realized through the adaptation of one side to the results of practical actions of the other (coadaptation). It should be noted that changing the protection paradigm does not mean denying the methods, technologies and mechanisms used by the parties at the previous stages of its development. But here the problem arises of balancing all these methods, technologies and mechanisms without exceeding the economically acceptable volume of total investments in the information security system. To resolve it, an adaptive approach to building an information security system is proposed, based on:

- the introduction of a set of verbal role models of typical scenarios of the attacker's behavior;
- the formation of reflexive risk models, which are mathematical models of risks for the above-introduced typical scenarios of the attacker's behavior, which take into account the characteristics of both sides of the information conflict;
- the use of reflexive risk models to calculate the basic indicators of the information security system, in particular, the estimated value of the maximum investment volume;
- harmonization of the financial and economic capabilities of the organization with its requirements and capabilities in the field of information protection, ensuring effective and rational investment in information security and the formation of its structure.

In the context of the results obtained in the work, promising directions for further research are: obtaining factual confirmation of the optimal ratio given in the work between the size of investments in information security and the possible level of losses in the absence of the necessary level of protection, taking into account the value of the protected resources and the potential of the attacking side, as well as forecasting impending changes of information security system paradigm, in particular, associated with the increase in the number of targeted ransomware attacks.

References

[1] A.Arkhipov, S.Arkhipova, Adaptive aspects of building information security systems, in: Proceedings of the 1st International scientific-practical conference Resources security of information systems, NUCHP, Chernihiv, 2020, pp. 37-43

[2] S.B.Lipner, The Birth and Death of the Orange Book, in: IEEE Annals of the History of Computing, 2015, vol. 37, no. 2, pp. 19-31. doi:10.1109/MAHC.2015.27

[3] O.Arkhypov, M.Gregus, Y.Arkhypova, Application of a risk-based approach using reflexive risk models in building information security systems, in: S. Pickl, V.Lytvynenko, M.Zharikova, V. Sherstjuk (Eds.), Proceedings of the 1st International Workshop on Computational & Information Technologies for Risk-Informed Systems, CITRisk-2020, vol. 2805 of CEUR Workshop Proceedings, Kherson, Ukraine, 2020, pp. 130-143. URL: http://ceur-ws.org/Vol-2805/paper10.pdf

[4] H.Behara, Economics of Information Security Investment in the Case of Simultaneous Attacks, in: Proceedings of the 4-th Workshop on the Economics of Information Security, WEIS 2006, Cambridge, England, 2006. URL: https://www.researchgate.net/publication/228612670_ Economics_of_information_security_investment_in_the_case_of_simultaneous_attacks.
[5] Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, Washington, D.C., 2017. URL: http://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf
[6] O.Arkhypov, Introduction to risk theory: information risks, Nats. SBU Academy, Kyiv, 2015
[7] Media.kaspersky.com, Advanced protection against sophisticated threats and risk reduction of targeted attacks, 2017. URL: https://media.kaspersky.com/ru/business-security/Kaspersky_Anti_Targeted_Attack_Platform_Whitepaper_RU.pdf
[8] R.Colbaugh, K.Glass, Proactive Defense for Evolving Cyber Threats, Sandia National Laboratories Albuquerque, New Mexico and Livermore, California, 2012. URL: https://fas.org/irp/eprint/proactive.pdf
[9] R.Wirtz, M.Heisel, CVSS-based estimation and prioritization for security risks. Paper presented at the ENASE 2019, in: Proceedings of the 14th International Conference on Evaluation of Novel Approaches to Software Engineering, 2019, pp.297-306. doi:10.5220/0007709902970306
[10] H.Bolivar, J.Parada, H.Roa, J.Velandia, Multi-criteria decision making model for vulnerabilities assessment in cloud computing regarding common vulnerability scoring system, in: Proceedings of the 2019 Congreso Internacional De Innovacion y Tendencias En Ingenieria, CONIITI 2019, 2019. doi:10.1109/CONIITI48476.2019.8960909
[11] K.Alperin, A.Wollaber, D.Ross, P.Trepagnier, L.Leonard, Risk prioritization by leveraging latent vulnerability features in a contested environment, in: Proceedings of the ACM Conference on Computer and Communications Security, pp.49, 2019. doi:10.1145/3338501.3357365
[12] Habr.com, Information security of bank non-cash payments, part 4, Overview of threat modeling standards, 2018. URL: https://habr.com/ru/post/351326/
[13] A.E.Arkhypov, Risk-based approach to evaluating the "reasonable" level of investment in information security systems, Legal, normative and metrological security of the information security system in Ukraine, Kyiv, Issue 1 (35), 2018, pp. 18-29
[14] A.V.Lukatsky, Detection of attacks, BHV-Petersburg, SPb, 2003
[15] W.Stallings, Network Security Essentials: Applications and Standards, 6th. ed., Prentice Hall, 2016.
[16] Media.kaspersky.com, Threats to the future: be prepared for them. Special Report on Advanced Threat Strategies, 2015. URL: https://media.kaspersky.com/pdf/ APT_Report_ONLINE_AW_rus.pdf
[17] O.Sedov (Ed.), Business Information Security. Targeted attacks – a marketing term or a sophisticated type of attack?, BISA, Moscow, №6, 2014. URL: https://www.twirpx.com/file/1636144/
[18] E.Hayden, The New Paradigm for Utility Information Security: Assume Your Security System Has Already Been Breached, in: The Industrial Control Systems Joint Working Group Newsletter, September 2011, ICSJWG Newsletter, 2011. URL:

https://www.fbiic.gov/
public/2011/sep/ICSJWG_Quarterly%20Newsletter_September%202011.pdf.
[19] Saini Hemraj, Saini Dinesh, Proactive cyber defense and reconfigurable framework for cyber security, International Review on Computers and Software, Vol.4. No.1, 2007. URL: https://www.researchgate.net/publication/288516946_Proactive_cyber_defense_and_reconfigurable_framework_for_cyber_security.
[20] R. Travis, Chief Information Security Officer best practices for 2018: Proactive cyber security, Cyber Security: A Peer-Reviewed J., Volume 1, Num. 4, 2018, pp. 361-367(7). URL:
https://www.ingentaconnect.com/content/hsp/jcs/2018/00000001/00000004/art00009#expand/collapse.
[21] K. Nakao, Proactive cyber security response by utilizing passive monitoring technologies, in: Proceedings of 2018 IEEE International Conference on Consumer Electronics (ICCE), 2018, pp. 1-1, doi: 10.1109/ICCE.2018.8326061.
[22] R. Marshal, K. Gobinath, V. V. Rao, Proactive Measures to Mitigate Cyber Security Challenges in IoT based Smart Healthcare Networks, , in: Proceedings of 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021, pp. 1-4. doi: 10.1109/IEMTRONICS52119.2021.9422615.
[23] P. Paganini, The Crimeware-as-a-Service model is sweeping over the cybercrime world. Here's why, 16 October 2020. URL: https://cybernews.com/security/crimeware-as-a-service-model-is-sweeping-over-the-cybercrime-world.
[24] Krasnov, Ordering a cyberattack is now no more difficult than pizza to the office, 2018. URL: https://rb.ru/opinion/tri-kiberataki.
[25] Tadviser.ru, Crime-as-a-Service, 2020. URL: https://www.tadviser.ru/a/551165.
[26] N. Grebennikov, Ransomware: how ransomware programs began to work according to the service model and what to do about it, 2017. URL: https://www.forbes.ru/tehnologii/342021-programmy-vymogateli-kak-ransomware-virusy-stali-rabotat-po-modeli-servisa-i-chto.