Application of a risk-based approach using reflexive risk models in building information security systems

Oleksandr Arkhypov[1][0000-0001-6832-2223] , Michal Gregus [2][0000-0002-8156-8962]

and Yevheniia Arkhypova[3][0000-0002-1640-1488]

[1] Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine
[1] sonet0515@gmail.com, [3]evgar55@gmail.com
[2] Comenius University in Bratislava, Bratislava, Slovakia
Michal.Gregus@fm.uniba.sk

Abstract. The risk-based approach (RBA) provides certain advantages in the construction and operation of information security management systems, therefore, the most frequently applied standards in this area are based on it. But the practical application of RBA for protection against cyber threats is fraught with a number of difficulties and limits. It is shown that application of a detailed risk assessment to assess the information security in organization intensively using the Internet and other IT in its activities, require a lengthy work to investigate vulnerabilities, calculating the private risks, reducing them into risks of threat. Taking into account the extremely high labor costs of this procedure, it is relevant to solve the problem by assessing high-level risks. Four verbal specifications of the attacker are introduced, describing various aspects of his behavior and skills, the socio-psychological context of his actions, the target settings of these actions, affecting the choice of the attacker's strategy, methods and ways to implement information threats. On the basis of these specifications reflexive risk models are formed. These are mathematical models whose structure and parameters reflect the characteristics of the attacker contained in its specification. Each of these models can be tailored to its own security policy to minimize losses to the organization. The study of reflexive models in a number of cases made it possible to determine the maximum volume of investments in the information security system and reveal the limitations in the application of the RBA to the construction of the information security system.

Keywords: risk-based approach, investments, reflexive risk models, hacker, information security, information security system.

1 Introduction

In modern society, information is one of the basic resources, the need to protect of which is recognized by the overwhelming majority of business entities. In these conditions, issues related to the protection of information that may be of interest to potential competitors, insiders, intruders, etc. are especially relevant. Taking into account

the specifics of information resources, including the difficulties arising when trying to evaluate them, as well as the limited financial resources, there is a need for an adequate assessment of the level of reasonable investments in the information security system of organizations that can be determined based on a risk-based approach.

Currently, there are some numbers of regulatory documents governing information security issues. They are the basis for creating systems for assessing both information risk and information security as a whole. The results of information risk evaluating affect the amount of funds invested in information security systems, therefore, one of the important conditions for the normal functioning of these systems is a reliable and accessible procedure for analyzing and assessing of information risks.

The risk-based approach provides certain advantages in the construction and operation of information security management systems, therefore, the most frequently and successfully applied international and industry standards in this area are based on it. Unfortunately, the practical application of risk-based approach for protection against cyber threats is fraught with a number of difficulties.

2 Related Works

Quite a lot of modern scientific papers are devoted to the research of various aspects of assessment and risk protection in information systems [1-3]. In particular, existing information risk assessment methodologies for identifying information systems strengths and weaknesses as well as assessing the information security risk level through the fuzzy logic apparatus are analysed in [1].

Some academic papers are devoted to deriving an organization's optimal level of information security investment, among which much attention is paid to the Gordon-Loeb Model (GL Model) and its modifications [4-5].

At the heart of the most frequently and successfully applied international and industry standards for Information security management systems (ISMS) is a risk-based approach (RBA), which provides some advantages in the construction and maintenance of those systems.

RBA is different significantly from the directive approach to building information security systems (ISS). The directive approach is based on the use of the recommended list of potential threats in terms of availability, integrity and confidentiality of information, which, as a rule, is fully used to form a system of security services when building an ISS. In contrast to directive approach, RBA allows highlighting from the huge number of existing threats and vulnerabilities of information systems (IS) those that are really relevant for the protection of information in a particular organization. This creates objective prerequisites for minimizing investment in information security. A detailed analysis of the mechanisms for the implementation of the limited range of actual threats makes it possible to choose the best methods and means of protection that really correspond to the level of protection guarantees. This allows you to form objective plans and evaluate investment budgets for the creation of ISS and ISMS. The found investment volumes are analyzed from the point of view of the effectiveness of the information security system, compared with the overall budget of the or-

ganization, etc. Based on the results of the analysis, the initially introduced levels of protection guarantees can be revised, corrected, re-planning and budgeting of ISS, i.e. the analysis procedure takes on an iterative nature.

The procedure for identifying a group of threats relevant to information security, which is the final stage of the risk assessment process, is called risk prioritization [7]. Risks prioritization in any area involves dividing them into levels, for example tolerable, low, medium, high and intolerable risks, which are usually determined based on the criteria of likelihood and impact / potential consequence [8; 9] or, for example, severity, occurrence and detection [10].

Prioritization of information risks, which are caused by the realization of possible information threats t_i, $i = \overline{1,n}$, involves, firstly, the identification of private risks for these threats:

$$r_i = p_{\text{ti}} q_i, \tag{1}$$

where p_{ti} is a quantitative assessment of the likelihood of the implementation of the corresponding information threat, and q_i is an assessment of losses caused by this threat. After that, it is required to rank the risks in the resulting set $\{r_i\}$ in descending order of their values and to select from the ranked series its left fragment containing significant for the organization risks. The threats that generate these risks form the group of the required actual threats.

On the basis of a group of significant risks (i.e. risks of actual threats), the value of the integral (generalized) risk R is formed. The integral (generalized) risk is calculated by multiplying the possible losses Q of the organization, which are the result of the combined action of all analysed actual information threats by the probability of these losses P_T, i.e.: $R = P_T Q$. Integral risk is a universal indicator of the degree of information security, which makes it possible to objectively assess the level of initial threats to information processed in the organization's IS, the level of residual threats (after building an information security system), and the effectiveness of the information security system. The following indicator is used to analyse the effectiveness of the information security system:

$$E = (R_1 - R_T)/c = \Delta_R/c. \tag{2}$$

Here R_1 is the initial value of the integral risk characterizing the possible losses of the organization due to the implementation of actual information threats in the absence of the information security system, R_T is the residual value of the organization's integral risk, which estimates possible losses after the introduction of the information security system, and Δ_R is the amount of possible losses that were prevented due to the establishment of an information security system in the organization.

Since the results of risk assessment affect the amount of funds invested in the information security system, the formation of an understandable and transparent process for analyzing information risks is the most important condition for the successful functioning of ISMS in the organizations. This also explains the strict requirements for the objectivity and accuracy of the calculated risk assessments.

The procedure for finding the integral risk in some cases may be quite simple. For example, subject to the independence and incompatibility of the actual threats and the independence of the consequences resulting from their implementation, the integral risk corresponds to the total risk $R = \sum_{i=1}^{n} r_i$. However, for organizations with a rather

complex structure, having a significant amount of information resources (IR) and intensively using complex information technologies in their work, it will be incorrect to calculate the integral risk as the total risk. In such cases, the integral risk should be calculated taking into account the possibility of the impact of several threats, including their joint implementation with the manifestation of interrelated, interdependent consequences, which is an extremely nontrivial task [11]. In such conditions the use of the total risk as an assessment of the integral risk usually gives a significantly overestimated estimate, contributing to an unreasonable increase in the volume of investments in the construction of ISS. In addition, in formula (1), when calculating private risks as values of p_{ti} and q_i, expert estimates are usually used, which introduces subjective errors into the calculated values, which reduce the reliability of the results of subsequent analysis. Another negative aspect of the risk assessment process described above is its duration and laboriousness, caused, in particular, by the iterative nature of the choice of the structure and configuration of the information security system (taking into account the need to use the integral risk indicator for each iteration, which does not have a general formalized procedure calculation). This approach to assessing information risks, due to its labor intensity and duration, is called detailed risk assessment.

The described above disadvantages of this approach stimulated the development of a more general approach called risk assessment of a high-level organization, which is given in the current state standards of Ukraine [12; 13]. In this more general approach, the technological aspects of risk assessment of the organization do not play a leading role; in particular, a detailed analysis of IS threats and vulnerabilities is not carried out. Instead, the emphasis is on generalized risk scenarios, the degree of dependence of the organization's business on the status of its information assets, in particular, on the overall level of the organization's investment in information security. This approach is focused primarily on solving general strategic aspects of information security: organizational, economic as well as basic technical issues.

If it is necessary to ensure the safety of especially valuable assets, a detailed risk assessment procedure is additionally carried out, which in this case is not iterative in nature and does not require the subsequent calculation of the integral risk through a set of significant private risks. This approach to risk analysis is called a combined approach [12]. It guarantees obtaining a full and technologically completed solution to the problem of building the organization's information security system after conducting a high-level risk assessment.

Note that the goals and methods of using RBA for the analysis and assessment of the organization's information security are not defined uniquely, much depends on the properties and characteristics of the organization itself. Of particular interest is the generalization of the known practical results of the use of RBA for solving information security problems, the formalization of procedures in which RBA is the basic methodology, the assessment of the prospects of RBA for protecting organizations from modern cyber-attacks.

3 Application of the RBA in the high-level risk assessment procedure

Let's apply RBA to assess the information security in an organization with a fairly complex regional structure, having a significant distributed information resource I, intensively using the Internet and other information technologies in its activities.

A preliminary analysis of possible threats to the information resources of this organization, carried out using the list of threats given in the ISO / IEC 27005 standard [13], allows to claim the following.

Nine out of 77 threats presented in the list are associated with the impact of natural phenomena (climatic, seismic, volcanic, meteorological and flooding), and of an accidental nature (hardware failure and equipment failures, software failures and errors). Effective decisions to minimize the risks associated with them can be made immediately only for these nine threats.

The remaining 68 threats represent the implementation of deliberate malicious acts aimed at information assets. The source of these threats is a person: a malefactor (intruder) or a group of malefactors. Note that the same threat can be implemented using different attacks (mechanisms) based on the use of various vulnerabilities of information systems of organizations. At the same time, the degree of success of the attack (i.e. the probable parameter risk) and the level of possible losses of the organization directly depend on the potential of the attacker – the competence, resources and motivation of the malicious [14].

It is obvious that the application of a detailed risk assessment in this situation will require a lengthy and painstaking work to investigate vulnerabilities and enumerate the attack mechanisms implemented on their basis, to find out the missing information for calculating the private risks of individual attacks, reducing them into risks of threat, etc. in accordance with the detailed evaluation procedure outlined above. Its intermediate result will be the calculation of a value R_1, a pair of values R_T, Δ_R for the proposed version of the information security system, evaluating the effectiveness of this version of the information security system, making adjustments and changes to it (in the mode of possible reusable iteration) and finally determining the acceptable (in accordance with the adopted system of criteria) investment amount c in the organization's information security system.

Taking into account the extremely high labor costs of this procedure, it is relevant to solve the problem by assessing high-level risks, excluding the use of an iterative procedure as well as without resorting to preliminary calculation of partial risks. It should be noted that such solutions have actually already been obtained in [6; 11; 15], although the problem statement there was somewhat different. In this regard, in the materials presented below, a number of results will be presented only with references to paper in which they are given.

We use the so-called two-factor formula to describe the integral risk:

$$R = P_T Q. \tag{3}$$

where the probability P_T of occurrence of losses Q is represented by multiplication

$$P_T = P_t P_v. \tag{4}$$

Here P_t is the likelihood of an attacker's motivation (his interest in the organization's information resource I, prompting him to commit any attacking actions aimed at this resource), P_v - the likelihood of a successful use of the organization's IS vulnerabilities by an attacker to implement his attacking actions. Structuring the probability P_T is convenient in that the probability of motivation P_t is actually determined only by the level of interest of the attacker to the information resource of the organization, which makes it expedient to find this probability in the form of a single expert assessment. One way to get this estimate is the using a heuristic dependence

$$P_t(g, D) = \frac{g-D}{g} = 1 - \frac{D}{g}, \quad (5)$$

where g is the value of the resource I for the malefactor (attacker), D is the generalized costs of preparing and implementing attacking actions by the attacker, presented in a monetary form, $g - D$ is the attacker's net profit in the case of a successful attack. Obviously, the higher is g, the closer to 1 the probability P_t. With a decrease g, in the case $g \leq D$ the attack becomes meaningless, unless the interests of the attacker go beyond commercial gain.

It should also be noted that there are two features that are important for the practical application of formula (5): the parameters included in expression (5) are determined only by the interests and motives of the attacker's behavior; the perceptions of the value of the same information resource by the attacking and defending sides is generally different – "asymmetric" [11; 15; 16]. For example, for the owner of a resource, its value q is usually calculated based on an analysis of the cost aspects of creating this resource, the calculation procedure is often typified, and the obtained estimates are quite stable. For the attacking side, the value g of the "extracted" information is formed on the basis of the market value of the resource and the number of potential buyers wishing to get it in their property. Thus, $g \neq q$.

The probability of a successful attack P_v is determined by the ratio of the potentials of the attacking and defending sides and can be represented by a next heuristic equation:

$$P_v(q, c, D) = \frac{\mu q}{\mu q + s\frac{c^z}{D}}, \quad (6)$$

where c is the total volume of investments in the organization's information security, $\mu = g/q$ is the coefficient of asymmetry in the perception of the value of information by the attacking and protecting sides, s is the coefficient that determines the level of efficiency of investments c in the information security: subject to the same investment volume c, the higher the value s, the lower the probability value P_v. The value of the coefficient s depends on the organization's attitude to information security issues and is determined by the level of maturity of the organization in the field of information security management. It is possible to obtain a quantitative (point) assessment of the level of maturity by applying the methodology described in [7] for self-assessment of the level of maturity of the risk management system in an organization. The score found by this method should be used as the desired value. The maximum possible value corresponds to 85 points, a high level of maturity of the organization is characterized by a range of 51 to 85 points.

It's obviously if an information resource I is not interesting for an attacker, in this case $g \to 0$, the coefficient $\mu \to 0$ as well as probability of a successful attack $P_v \to 0$. On the contrary, if the resource I is of no value to the organization owner, there are practically no investments in the information security system ($c = 0$), and $P_v = 1$. Finally, if the attacker is extremely interested in the resource I and is ready to receive it at practically unlimited costs, in this case $\to \infty$, $P_v = 1$.

Substitution of expressions (5), (6) into formula (3) makes it possible to construct a formalized generalized model of integral risk

$$R(c) = \left(1 - \frac{D}{g}\right) \frac{\mu q}{\mu q + s\frac{c^2}{D}} q, \tag{7}$$

in which the value c is included as one of the parameters, and then make in general form the dependence of the prevented losses $\Delta_R(c)$ on the level of investment in the organization's information security system.

To conduct research within the framework of a high-level risk analysis, we will define the concept of the organization's information security system efficiency. We will assume that the fulfillment of the condition $\Delta_R(c) > c$ is obligatory for an effective ISS. Then we will consider the most effective ISS for which the difference $\Delta_R(c) - c = \Delta_c(c)$, representing the "net profit" due to the construction of the ISS, seems to be the largest. The effective volume of investments in this case will be [11, 15]:

$$c_{\text{eff}} = \underset{c \in C}{\operatorname{argmax}} \Delta_c(c), \tag{8}$$

where C is the set of values c for which $\Delta_R(c) > c$. Unfortunately, the use of the generalized integral risk model (8) does not allow finding c_{eff} explicitly in the analytical form. However, in a number of cases, applying a more detailed description of the capabilities and properties of the attacking side, the motivational and economic aspects of its behavior, it turns out to be real to obtain an analytical solution to the optimization problem (8) and much information that complements this solution.

4 Reflexive risk models

Now we will consider four verbal specifications of the attacker, reflecting various aspects of the behavior and preparation of the attacker, social and psychological context of its actions, the existing (often prescriptively determined) target settings for these actions, which largely affect the choice of an attack strategy, methods and ways of information threats implementing. According to the introduced specifications, reflexive risk models are formed. Each model has certain features depending on the characteristics of the attacker.

4.1 Specification 1. Script kiddie (newbie, lamer)

The attackers are inexperienced persons that do not have main skills in information security system. They often lack the sufficient knowledge to write an exploit or their own program, so they use scripts or software developed by others [17; 18]. Script

kiddies usually do not understand the mechanism of attack action as well as have little idea of it potentially consequences. They are not capable of independently implementing effective attack solutions because have lack of experience and financial resource. The purpose of script kiddies can be to impress their peers, to have fun, to be accepted by "serious" hackers group [18]. Nevertheless, some researchers and practitioners in the field of information security consider that script kiddies can cause significant damage to the ISS: they are very numerous and some of them are quite stubborn and persistent in their attempts to implement the attack. In particular, Lloyd Borrett, notes that an increasing number of script kiddies are motivated by the opportunity to make money, because the cost of simple hacking scripts is relatively low.

Since script kiddies are the most common type of intruder, the need to protect against it is a top priority when building an information security system It should be emphasized that the "old", unoriginal threats implemented by script kiddies can cause very significant damage to the organization if it does not pay due attention to protecting your information. In addition, it should be noted that script kiddie community is not homogeneous, and those of them who have gotten a good education and are able to learn can become advanced cybercriminals.

In general, we will assume that the following conclusion is true regarding script kiddies. First, the attacking activity of script kiddies is not purposeful, the objects of their attacks are random computers, and various random information (although sometimes very valuable) falls into the hands of the attacker. In this regard, their motivation is extremely unstable and spontaneous so formula (5) is not relevant for script kiddies. Second, the script kiddies are not able to independently develop the means and new attack mechanisms, moreover, they do not understand the mechanism of action of the old ones, basing their actions in the implementation of threats mainly on the application of the enumeration principle. Therefore, the basic level of security, which is competently embodied in the organization's information security system, focused on the use of means and methods of protection against already known "old" threats, is quite effective for countering attacks by the script kiddies.

This conclusion corresponds to a reflexive risk model of the form:

$$R(c) = P_t \frac{q}{q+\mathrm{sc}} q, \tag{9}$$

where the probability of a successful use of an organization's IS vulnerabilities by an attacker to implement his attacking actions is determined by

$$P_v = \frac{q}{q+\mathrm{sc}}, \tag{10}$$

It follows from (10) that the information security in an organization primarily depends on internal parameters: the amount of investments c in the ISS, the level of organization maturity (determined by the value of the parameter s) and the value q of its information resource. An increase of the values c and s leads to a decrease in the values of probability (10).

Having calculated for the reflexive risk model (9) the value of prevented losses $\Delta_R(c)$ and, compared it with the volume of investments c in the information security system, we find the "net profit" of the organization due to the construction of the ISS:

$$\Delta_{\mathrm{c}}(c) = \Delta_R(c) - c = \frac{\mathrm{sc}}{q+\mathrm{sc}} P_t q - \mathrm{c}, \tag{11}$$

Analysis of expression (11) allows determining [6; 11] the range of "reasonable" investments $0 \le c \le q(s-1)/s$ within which $\Delta_R(c) > c$. Here is the formula for calculating the effective volume of investments:

$$c_{\mathrm{eff}} = \frac{q}{s}(\sqrt{P_t s} - 1), \tag{12}$$

as well as formulas for calculating the value of the probability . P_v and risk R under the conditions of an effective investment volume:

$$P_v(c_{\mathrm{eff}}) = \frac{1}{\sqrt{P_t s}},\ R_T(c_{\mathrm{eff}}) = P_v(c_{\mathrm{eff}}) P_t q = q\sqrt{\frac{P_t}{s}}., \tag{13}$$

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 one-extreme character with a maximum: $\max[c_{\mathrm{eff}}(s)] = 0{,}25\mathrm{qP}_t$ [11, 15]. Obviously, the largest value of effective investments in ISS will be at $P_t = 1$, while the maximum investment in ISS will be $c_{\mathrm{effmax}} = 0{,}25q$, i.e. 25% of the cost of the resource q, which is the object of protection. For highly effective security solutions (for example, $s = 60$) in accordance with formula (12), even with $P_t = 1$, the volume of investments in the ISS can be at the level of 11-13% of the cost of the protected resource. The obtained results are in good agreement with the empirical estimates of the volume of investments given in a number of publications the authors of which focus on the amount of 15-20% of the value of IS assets.

It should be noted that as well as script kiddie the various network infections and worms, excluding zero-day attacks, can be successfully eliminated at the basic level of protection.

4.2 Specification 2. Professional Hacker

The attacker is represented by a professional or a group of professionals with the necessary knowledge, skills and sufficient experience, for which hacking is the main activity of a frankly commercial nature. A professional hacker usually has some financial and economic resources, but for him, nevertheless, the limitation $D \le g$ remains quite relevant. If the cost of the information resource I is estimated by the sides of the attack and defense approximately the same, i.e. the asymmetry coefficient $\mu = 1$, the reflexive risk model for this case will be as follows:

$$R(\mathrm{c}) = (1 - \frac{D}{g})\frac{q}{q+s\frac{\mathrm{c}^2}{D}} q, \tag{14}$$

The research of formula (14) for $D = 0$ allows to estimate the boundary values of the range of reasonable investments: $0 \le c \le q$. With increasing values of D, for $D \to 0{,}25\mathrm{sqP}_t^2$ the right and left boundaries of the range approach, contracting to the point $c = \frac{\mathrm{qP}_t}{2}$ for $D = 0{,}25\mathrm{sqP}_t^2$. In this ultimate case, the largest investment in the information security system will be $c_{\mathrm{effmax}} = 0{,}5q$, i.e. 50% of the cost of the resource

q [11, 15]. The expenditure of this volume of investments requires an analysis of possible threats to information security, the identification of actual threats, the implementation of a protective measures system in the form of an integrated information security system (IISS) under conditions of optimal allocation of investments.

As noted above, the attacker can invest significant funds in organizing and conducting an attack, comparable in magnitude to the value of q, but as a rule the allocated attack potential does not exceed the limits of economic feasibility. However, in the case $\mu >> 1$, i.e. with a significant asymmetry in the perception of the value of information by the attacker and defender, a situation arises that can be defined as a long-term targeted attack. At the same time, the attacking side, which has previously allocated hefty resources for preparing the attack, but has not yet achieved success, switches to wait-and-see tactics, accompanied by constant monitoring of the quality of the functioning of the attacked organization ISS. Sooner or later, in the event of a local decrease in the level of its security (the appearance of even a short-term vulnerability), the attacker carries out a successful attack. In this case, the attacker's main expendable resource is his time and the costs of monitoring the security status of the attack object.

From the formal point of view, if $\mu \neq 1$, when $g \to \infty$ the probability of the threat activation is $P_t \to 1$, i.e. the threat exists constantly and its implementation will occur as soon as the opportunity presents itself. If there is an insider in the attacked organization, he can report the onset of this moment or try to create it. This moment will correspond to a local burst of probability P_v, which, according to the definition introduced in [11], is a "terminal" probability, the value of which changes over time in accordance with the chosen attack tactics. In this case defensive side should choice a strategy of so-called proactive defense, based on the research of the behavior, tactics and strategy of the attacking side, i.e. used the approaches and principles of reflexive control [19]. Proactive defense strategy allows defensive side to postpone the onset of the moment of successful implementation of the threat theoretically for an unlimited period of time.

Thus, the IISS, built only in accordance with the requirements of the current regulatory documents of the ISS system, does not provide sufficient guarantees of protection against attacks in cyberspace implemented today: targeted advanced persistent threats, advanced evasion techniques. The complexes of protective measures used today are young effective against these threats. In this regard, the development of proactive defense systems using the approaches and principles of reflexive control is promising.

4.3 Specification 3. Hired professional executor

The attacker, in order to achieve his goals, resorts to the services of a hired contractor who is obliged to do his job under any circumstances. In particular, if his task is to implement any information threat, the professional executor immediately proceeds directly to the search and exploitation of the vulnerability of the organization's IS, i.e. it is obvious that in this situation $P_t = 1$.

In the previous specifications the attacking side in its actions is guided by the principle of economic expediency (reasonable sufficiency).

Unlike them, a feature of specification 3 is that due to the special importance of the task assigned to the professional executor, resource constraints are removed and, moreover, he can count on attracting various additional resources to support his actions: financial, technical, operational as well as information and analytical etc.

In practice this means the possibility of implementing very high-cost attacks (D → ∞) within the framework of Specification 3. A typical example of such situation is the implementation of a particularly important task by an undercover man who is a professional trained to carry out attacking actions in cyberspace [15; 19].

The reflexive risk model for this case is simple:

$$R = P_v q = \frac{q}{q + s\frac{c^2}{D}} q, \tag{15}$$

It is obvious that with the removal of resource constraints ($D \to \infty$) the probability $P_v \to 1$, i.e. the successful implementation of the threat by the attacker is practically guaranteed and, as a result, $R(c) \to q$. This is achieved through the implementation by the attacker of new original attacks, protection from which is almost impossible to envisage within the framework of the standard RBA methodology presented in the current risk management guides, based on the research and analysis of previous security incidents.

4.4 Specification 4. Hacktivist

The attacker is an ideological hacker who use computer systems for a politically or socially motivated purpose [16; 17; 19].

He seeks to transfer the promotion of political or social ideas (often of a rather dubious nature) to cyberspace, organizes actions of civil "electronic" disobedience in cyberspace, trying to attract the attention of the authorities and the public (sometimes in a rather tough form) to certain issues and problems of modern society through the synthesis of social activity and hacking. The most typical hacktivists actions are website defacement and computer hacking, in particular denial-of-service attacks, e-mail bombing as well as computer viruses and worms.

There is practically no commercial component in the actions of a hacktivist, his attack potential, in particular resource provision, is usually limited, therefore Specification 4, depending on the resources available to the hacktivist, may be close to Specification 1 or 2. Having established that the hacktivist belongs to a particular protest community, it is possible with a high degree of probability to assume the type, duration, mass, intensity and possible consequences of hacker attacks. Therefore, the use of ROA in such situations can be quite effective.

5 Conclusions

The analysis of reflexive risk models shows that they are focused on a certain set of attacker properties, which forms specific aspects of its behavior, the social and psychological features and target settings of its actions, which largely affect the choice of the attacking strategy, and methods of threats implementing. Each of these models can be tailored to its own security policy to minimize losses to the organization. Development of these security policies determines the content of an adaptive approach to managing the information security process in an organization. At the same time, "adaptive management" [19] refers to the process of applying a targeted choice, and, if necessary, changing the parameters and structure of the organization's ISS in order to make adequate decisions to ensure the required level of protection of its information resource from attacking actions of an intruder, harmonizing the financial and economic capabilities of the organization with its requirements and opportunities in the field of information security, ensuring effective and rational investment in the organization's information security system.

The study of reflexive risk models, reflecting for a number of typical "attack-defense" situations the characteristic features of the behavior and actions of the attacker, presented in the Specifications 1, 2 and, 4 (script kiddie, professional hacker, hacktivist), makes it possible to analyze high-level risks, predict estimates of the marginal volume of investments in the organization's information security, prioritize risks and identify a group of relevant information threats, thereby ensuring an effective distribution of funds invested in the organization’s information security.

An analysis of the application of RBA to building an organization's information security system using the risk model defined in the Specification 2 (Professional hacker) for long-term targeted attacks leads to the conclusion that it is impossible to provide sufficient guarantees of protection against a number of attacks, implemented in cyberspace.

Considering that the basic methodology of RBA, presented in the information security risk management standards, is based on the research and analysis of previous security incidents, the successful use of RBA to build an effective information security system that allows reflecting new, unpredictable attack history is not possible. In this regard, the use of RBA for building an information security system against hired professional executor (Specification 3) is useless.

References

1. Yevseiev, S., Shmatko, O., Romashchenko, N.: Algorithm of information security risk assessment based on fuzzy-multiple approach. Advanced information systems. 3, 2, 73–89 (2019). doi: 10.20998/2522-9052.2019.2.13
2. Butusov, I., Romanov, A.: Methodology of security assessment automated systems as objects critical information infrastructure. Voprosy kiberbezopasnosti [Cybersecurity is-

sues]. 25, 2–10 (2018). Doi: 10.21681/2311-3456-2018-1-2-10 . https://cyberrus.com/wp-content/uploads/2018/05/02-10-125-18_1.-Butusov.pdf
3. Buchyk, S., Shalaev, V.: Analysis of instrumental methods for determining information security risk information and telecommunication systems. Knowledge-based technologies, 3(35), 215–225 (2017).
4. Gordon, L., Loeb, M., Lucyshyn, W. and Zhou, L. Empirical Evidence on the Determinants of Cybersecurity Investments in Private Sector Firms. Journal of Information Security, 9, 133-153 (2018). Doi:10.4236/jis.2018.92010.
5. Gordon, L.A., Loeb, M.P. and Zhou, L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. Journal of Information Security, 7, 49-59 (2016). https://doi.org/10.4236/jis.2016.72004
6. Arkhypov, O.Ye., Arkhypova, Ye. O.: Features of the definition of the volume of investment in protection of information resources. Investment: Practice and Experience, 11, 71-74 (2015).
7. A guide to managing security risks. Microsoft Solution Development Group for Security and Compliance, Regulatory Standards and Microsoft Security Center of excellence. http://infoeto.ru/download/rukovodstvo-po-upravleniyu-riskami-bezopasnosti.doc
8. Software Risk Management: A Practical Guide, https://www.energy.gov/sites/prod/files/cioprod/documents/Risk_Management.pdf.
9. 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). http://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf
10. Sellappan, N., Palanikumar, K. Development of Modified Evaluation and Prioritization of Risk Priority Number in FMEA. International Journal of Engineering. 7, 1, 32–43 (2013).
11. Arkhypov O. Introduction to risk theory: Information risks. Kyiv, Nat. Acad. SBU (2015).
12. DSTU ISO / IEC TR 13335-3: 2003 Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security. – Kyiv, Derzhspozhyvstandart of Ukraine (2005). – III. 76 p.
13. DSTU ISO / IEC 27005: 2015 Information technology -- Security techniques -- Information security risk management – Kyiv, UkrNDNTS (2016).
14. GOST R ISO / IEC 15408-1. Information technology. Methods and means of ensuring security. Criteria for assessing the security of information technology. Part 1. Introduction and the general model.
15. Arkhypov A.E. The use of economic and cost models of information risks for assessing the limits of investment in information security. Zahist Informatsii, 17, 3, 211-218 (2015). http://ceur-ws.org/Vol-2608/paper14.pdf
16. Arkhypov, O.Ye., Arkhypova, Ye. O.: Risk approach for determining limit values of the level of investment in information security. Information security of man, society, state, 2 (18), 61-70 (2015).
17. Yermalovich, P., Mejri, M.: Ontology-based model for security assessment: Predicting cyberattacks through threat activity analysis. International journal of network security & its applications. 12 (2020), https://ssrn.com/abstract=3623746
18. Nycyk, M.: The new computer hacker's quest and contest with the experienced hackers. International Journal of Cyber Criminology (IJCC). 10(2): 92–109 (2016). DOI: 10.5281/zenodo.163402/

19. Arkhypov, A.., Arkhipova, S.: Adaptive aspects of building of information security systems. In: Proc. of 2020 Ist International conf. on Security of information systems resources, pp.37-43, Chernihiv (2020).