Vulnerability Analysis for Dynamic Investment Management

N. Lukova-Chuiko, R. Prus*

Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
*Corresponding author. E-mail: ruslana_prus@meta.ua

Paper received 17.04.15; Accepted for publication 16.05.15.

Abstract. The paper presents analysis of mathematical model and methodology of determining the optimal investment allocation between the objects of information security. The model allows to evaluate the potential losses decrease as a result of decisi on about investment allocation between information security objects. To predict the effectiveness of countermeasures and evaluate its work the model takes into account the vulnerability of objects to a security breach and potential loss due to such breach. Vulnerability function depends on the size of investment of both sides, can describe various systems, and includes the parameters that enable to identify the areas of greatest economic expediency of investment in complex information security systems. To coordinate the process of decision-making developed methodology of dynamic investment management. The main point of methodology is investment allocation conducted after identifying attacker's ways of threat realization. A dynamic confrontation is demonstrated on the system consisting of two objects. Analytical modeling of the process of defence and attack on the information security objects demonstrates that the methodology by taking into account attacker actions and vulnerability function raises investment usage efficiency and enables to assess the outcome of decisions.

***Keywords**: IT security, mathematical model, vulnerability, security breach, optimal security investment*

Introduction. Nowadays, when cyberwar became real, the issue of information security attracts more and more attention. Still decisions about the respective defence measures are mostly taken based on heuristics and experience and often subjective. Also because of lack of resources information security became a matter of economic incentives for risk management. Optimal deployment of investment in information security system allows to improve the level of information security and can help to reason whether some security measures are worth its cost [1,2]. In order to achieve this kind of functionality, methodology of dynamic investment management based on game-theoretic model is proposed [6].

The purpose of research was to analyse the impact of potential decisions made by attackers and defenders and respective effect on variation of system indices and characteristics. Analysis enables to estimate potential losses due to security breaches.

Materials and methods. Developed approach is focused on decision-making about information security system improvement by optimal investment allocation. Decision-making is the process of choosing most preferable option from the set of acceptable options. The problem is solving on the basis of knowledge about security system, all the processes taking place in the system and could happen in near future, also on the basis of calculated decision efficiency and quality indices. Therefore adequate model of the process of decision-making results implementation is needed. To run the analytic modeling of the process of defence and attack on the information security objects game-theoretic model of dynamic investment management is used. The model not only takes into consideration attacker actions but also makes it possible to assess the consequences of decisions, to prognose the value of potential losses and to choose that option that guarantees expected losses due to security breaches to be minimal in most adverse conditions.

Selection and justification of mathematical models play a key role in the study of information confrontation. Conventional image that creates a model must satisfy two conflicting requirements: in the greatest extent reflects the properties of the objects, their relationships and situations that arise in various forms of opposition, and at the same time avoids unnecessary complications, which can lead to significant computational challenges. While it is important to adhere to the system approach which in the problems of information security is manifested in the fact that the system "attack-defence" is seen in the interaction of its components according to their parameters and characteristics. Definition of these variables in the dynamic mode is complicated by a number of reasons. Primarily, it is the uncertainty of the conditions confronting, i.e. the impossibility of accurately predicting the intentions, capabilities and activities of the opponent, which is largely due to the lack of statistical data. Difficulties arise even in determining the parameters and characteristics of its own information system, for example, such an important indicator as vulnerability objects.

In order to estimate the optimal option of investment allocation between information security objects the function that measures the potential losses due to realization of threats is used [3]:

$$i(x,y)=\sum_{k=1}^{l} i_k(x,y)=\sum_{k=1}^{l} g_k f_k(x_k,y_k) \qquad (1)$$

where $k=\overline{1,l}$: object number; x_k i y_k: attacker investment to breach the system and information security investment to protect from that breach, respectively, $\sum_{k=1}^{l} x_k = X$, $x_k \ge 0$, $\sum_{k=1}^{l} y_k = Y$, $y_k \ge 0$; g_k: information value; $\sum_{k=1}^{l} g_k = 1$; $f_k(x_k,y_k)$: object vulnerability function of attacker-defender investment ratio.

Proposed model allows to evaluate the potential losses decrease as a result of decision about investment allocation between information security objects. As the result of alternating decision-making consequences modeling in dynamic mode optimal set of decision by both subjects, that in Game Theory present Nash equilibrium, is obtained.

Vulnerability function of objects, depending on the size of investment of both sides and can describe various systems, is used in modeling. Vulnerability functions include the parameters that enable to identify the areas of greatest economic expediency of costs in complex sys-

tems of information protection that allows to increase the efficiency of investments [4, 7].

Most crucial part of the modeling is vulnerability function estimating. It is denoted that with increasing security investments it is possible to decrease the vulnerability level and with increasing attacker investments it is possible to increase the vulnerability level. Therefore variables x_k, y_k in function $f_k(x_k, y_k)$ expressed as x/y relation. Also by security investing larger and larger amounts it is possible to make the attack probability arbitrarily small: $x/y \to 0$ $f(x,y) \to 0$ and vice versa: $x/y \to \infty$ $f(x,y) \to 1$. Under existing conditions next function may be used:

$$f(x,y) = \frac{\left(x/y\right)^n}{\left(x/y\right)^n + c} \qquad (2)$$

where parameters n, c differ for various security measures (Fig.1).

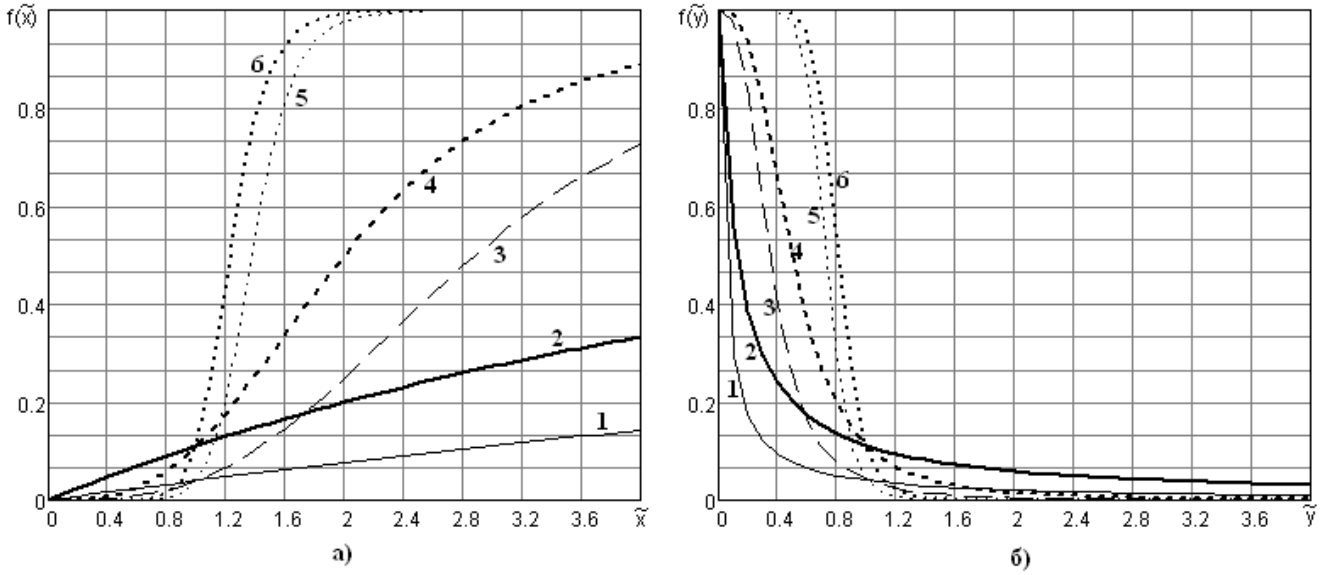

Figure 1. Vulnerability functions: a) dependence on *x* (*y* – const); б) dependence on *y*, (*x* – const) with various *n* and *c*: traces **1,2** – $n=1$, **3,4** – $n=3$, **5,6** – $n=10$, traces **1,3,5** – $c=24$, **2,4,6** – $c=8$

Linear-fractional ($n=1$) functions (2) represents information vulnerability of material information carrier. For such a class of functions insignificant increasing of security investments cause gradual small decreasing of the vulnerability level. Nonlinear-fractional ($n>1$) functions represent properties of information in computer systems. In this case for successful breach attacker needs substantial investments. With increasing of nonlinearity regarding factor n function $f(x,y)$ becomes step curve. This relation occurs in encryption: for successful breach attacker applies substantial investments, as a result potential losses due to realization of threats rise unevenly.

As example of determining parameters n and c results of reliability network system modeling were used [5]. On fig. 2 trace 1 represents reliability, trace 2 – vulnerability (assuming both characteristics are opposite).

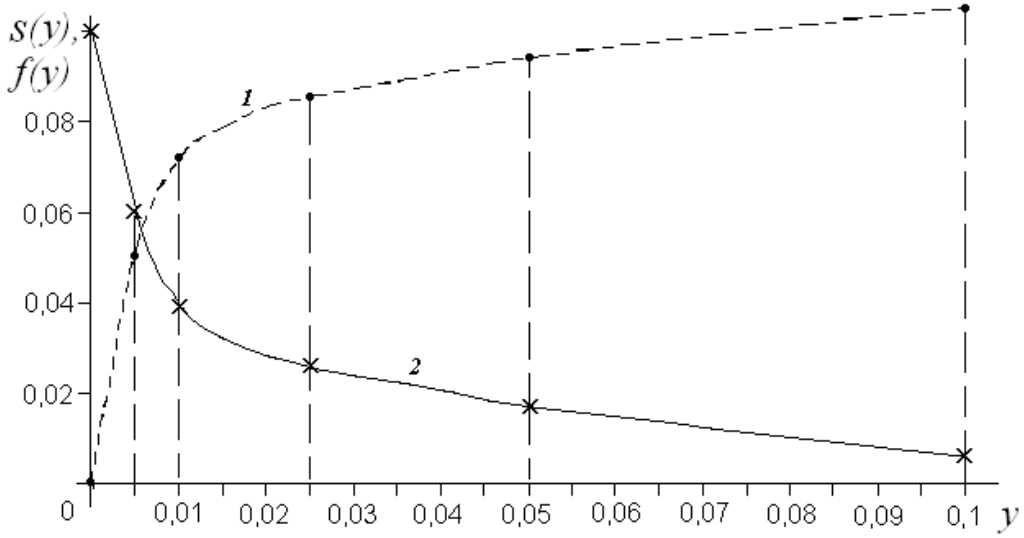

Figure 2. System reliability $S(y)$ (trace 1) and system vulnerability $f(y)$ (trace 2), y – expressed in per cent to g

Curve shape indicates that vulnerability can be approximated by function (2) with $n=1$. Parameter c was found by calculating c_i for every reference point and averaging these values minimizing total deviation. By computing value c = 1500 vulnerability function can be built:

$$f(y)=\frac{1}{1+1500y}$$

Although vulnerability function in this example was generated, for every particular element of the information security system function must be built using reliable empirical data which are limited. To gather data on information security incidents and analyse them regular monitoring of events and incidents must be provided. Also the majority of organizations might not disclose the information security incidents even if the data exists.

The vulnerability of computers, servers, networks, network equipment and software are detected, identified and classified during analysis. Analysis of vulnerabilities enables to predict the effectiveness of countermeasures and evaluate their work. It is created a database that contains all the necessary information for the verification of the system for the presence of gaps in the security system, anomalies in the network, and potential ways of penetration into the system through the software flaws.

System analysis of vulnerabilities is effective if the conditions are met:
– information about new vulnerabilities is constantly updating;
– while identifying of vulnerabilities the number of false positive results is less than the acceptable value;
– ability to check multiple systems simultaneously;
– results of inspections are presented in consistent, clear and understandable reports;
– recommendations for countermeasures to eliminate vulnerabilities are given.

The analysis of vulnerabilities consists of the following steps:
– identification and classification of site networks or systems;
– evaluation of the importance of each object;
– determination of potential threats, sources of their origin (at this stage the system is exposed to deliberate attacks to identify vulnerabilities);
– developing of the plan to fight off the most dangerous threats in the first place;
– implementation of measures to minimize damage caused by threats.

In order to conduct effective analysis of vulnerabilities security monitoring is held. Attention focuses on the most critical objects and it is enhanced of countermeasures to prevent the occurrence of threats. Investigation of the information security incidents is also conducted.

As much as credible vulnerability function will be built, as easier it will be to coordinate countermeasures against threats to lower the vulnerability. It is also critical in the aspect of rapid evolvement of threats to information system. Recently, many attackers to guarantee successful breach conduct espionage. Usually with growing awareness of system details intruder might redirect his attacks which might be followed by relocation of investments. Such actions must be answered by relocation of information security investments, respectively. To coordinate the process of decision-making under these conditions developed methodology of dynamic investment management. The main point of methodology is investment allocation is conducted after identifying attacker's ways of threat realization.

A dynamic confrontation is demonstrated on the system consisting of two objects (Fig. 3) characterized by different vulnerability functions and which vary in information value.

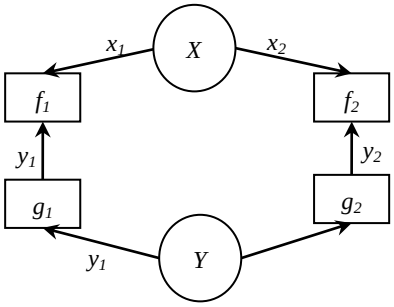

Figure 3. Security system scheme

Using game-theoretic regulations ensures that optimal decision about investment allocation will guarantee minimal potential losses under any most unfavourable actions of the attacker. Combining this with taking into account vulnerability function methodology reveals how investments in information security countermeasures influence the potential losses due to realization of threats. By using this methodology outcome of the optimal decision in unsettled conditions can be estimated.

Within the framework of methodology process of making moves in turn by attacker and defender is modeling (Fig. 4). It is assumed each of them knows investment allocation of his adversary after previous move and relying on this knowledge redirects his investments. Every decision is made by using objective function (1) and minimax criterion for defender or maximin criterion for attacker. Defender stops the process if next move is disadvantageous.

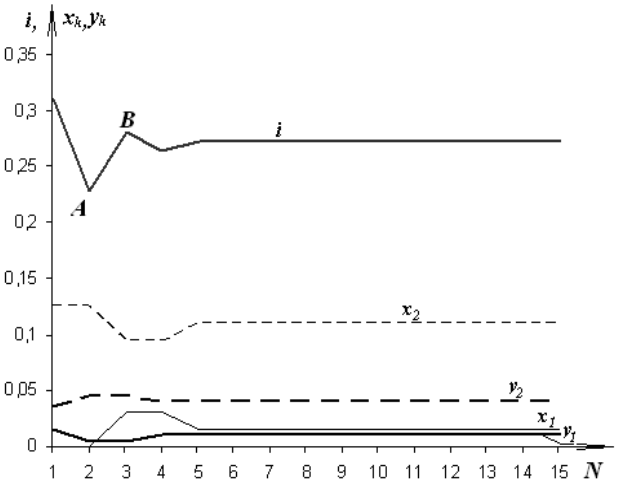

Figure 4. Dynamic confrontation of defender and attacker:
g_1=0,3; g_2=0,7;

$$f_1(x,y)=\frac{x/y}{x/y+8}; \qquad f_2(x,y)=\frac{\left(x/y\right)^2}{\left(x/y\right)^2+16}$$

Search for optimal information security investment allocation $\{y_k^0\}$ which guarantee minimal potential losses due to realization of threats with initialized attacker and defender investments $\sum_{k=1}^{l} x_k = X$ and $\sum_{k=1}^{l} y_k = Y$, respectively, is conducted in next sequence:

1. Information security investment allocation $\{y_k\}$ is initialized proportional to information value $\{g_k\}$.
2. Vulnerability functions (2) with appropriate parameters n and c are generated.
3. Values of objective function (1) for each option of attacker's investment allocation $\{x_k\}$ are calculated.
4. Using Bellman's method optimal attacker investment allocation $\{x_k\}$ for initialized investment allocation $\{y_k\}$ by maximizing potential losses $i(x)$ is found.
5. Considering attacker investment allocation $\{x_k\}$ found on previous step defender investment allocation $\{y_k\}$ by minimizing potential losses *i(y)* is adjusted.
6. Described procedure (steps 4-5) is repeating until $\max i(x)$ reaches its minimal value (Fig. 4). Consistent with criterion defender investment allocation $\{y_k^0\}$ is considered optimal.

Results and their discussion. Results of analyzing Fig. 4 follow. With total sum of investments ratio $X/Y = 2{,}5$ on first steps close to oscillating process, that describes redirecting of entire each side's investments from one object to another, takes place. It is often explained by limitation of attacker investments. In order to succeed in system breach for attacker more appropriate decision is to concentrate entire investments on the one object than to allocate them to several objects.

Defender keeps track of possible actions of the attacker and directs information security investments at the attacked object. Notched line *i(n)* on Fig. 4 shows that each step of the attacker raise the potential losses (point B) and each defender's step lower them (point A). Also on the second step ($N = 2$) all the defender's investments concentrated on the second more valuable object. On the next step ($N = 3$) rational attacker, assuming he improved his knowledge from outcome of the previous decision, to the second more protected object allocates less investments due to the lack of them. As countermeasure on the fourth step ($N = 4$) defender increases amount of investments in the first object security. Such defender's investment allocation ($y_1^0 = 0{,}01$; $y_2^0 = 0{,}04$) is optimal since together with attacker's decision ($x_1^0 = 0{,}015$; $x_2^0 = 0{,}11$) on the next step satisfies the requirements of the saddle point. Potential losses due to realization of threats equal $i = 0{,}166$. Any deviation from optimal decision is unprofitable since it guarantees the best result for each side under any actions of the adversary.

For efficient appliance of the proposed model should be used a reliable system of monitoring mechanism of information security incidents and alert mechanism of attack. Application of a reliable system of monitoring information security incidents and attacks notification mechanism reduces uncertainty and improves the accuracy of calculations, since it furthers the proper selection constraints and decision criteria, correct formation of the acceptable alternatives set, and proper evaluation of system parameters and characteristics, which increases the efficiency of the decision.

Monitoring of incidents, which include gathering, processing, transmission and analysis of data about the system, becomes the key element in justifying decisions. The primary task of monitoring is timely identification of the incident, its analysis and quick response.

The introduction of new ways of identification of events as deviations from the norm will help confirm the presence of incidents and timely and promptly respond to them and in some cases prevent attacks from intruders.

Incident response process can be organized as follows:

1) defining of information security incident, creating a list of events that classified as incidents;
2) notification of responsible person about the incident;
3) eliminating of the consequences and causes of the incident;
4) procedure for investigating the incident (determining of the causes of incident, the procedure for collecting and preserving evidences);
5) implementation of rehabilitative and preventive actions based on the results of the modelling of the process of defence and attack by using function (1).

Conclusions. Analytical modeling of the process of defence and attack on the information security objects demonstrates that this methodology of dynamic investment management by taking into consideration attacker actions raises investment usage efficiency and enables to assess the outcome of decisions, to prognose the value of potential losses and to choose that option that guarantees expected losses due to security breaches to be minimal under most unfavourable actions of the attacker.

Developed methodology provides reasonable results to support decision about optimal information security investment allocation between elements of information system, which differ in vulnerability, information value, and quantity of elements. By using vulnerability function methodology reveals how investments in information security countermeasures influence the potential losses and, at the same time, makes it possible to allocate investments to those elements of the system that minimize potential losses with highest efficiency of attack neutralization.

In order to fulfill effectively all these tasks, reliable monitoring system of information security events and incidents as much as mechanism for attacks alerting must be provided. Monitoring of information security incidents includes collecting, processing, signaling and analyzing data about system and becomes key point in decision-making process. On monitoring results depends how reliable input data such as vulnerability function, possible total amount of attacker's investments, and preferable ways of threat realization. At the same time, accuracy of the input data guarantees countermeasures to be operative, appropriate and quick.

REFERENCES

[1] Anderson, R., Moore, T. The Economics of Information Security // Science. – 2006. – Vol. 314. – No. 5799. – P. 610-613.

[2] Gordon, L.A., Loeb, M.P. The Economics of Information Security Investment // ACM Transactions on Information and System Security. – 2002. – Vol. 5. – No. 4. – P. 438-457.

[3] Levchenko, E., Rabchun, A. Optimization Problems of Information Security Management // Modern Information Security. – No. 1. – P.16-23.

[4] Levchenko, E., Prus, R., Rabchun, D. Economic Expedience Indices of Information Security Investment // Information Security. – 2012. – Vol. 18. – No. 2. – P. 6-11.

[5] Moitra ,S. Konda, S. A Simulation Model for Managing Survivability of Networked Information Systems // Technical Report CMU / SEI – 2000. – TR – 020, Dec. 2000.

[6] Prus, R. Optimal Security Investment Allocation in Dynamic Mode // Information Security. – 2012. – Vol. 18. – No. 1. – P. 26-32.

[7] Lui, W., Tanaka, H., Matsuura, K. Empirical-Analysis Methodology for Information Security Investment and its Application to a Reliable Survey of Japanese Firms // Information Proceeding of Japan Digital Courier. – 2007. – Vol. 3. – Sept. 2007. – P. 585-599.