Modeling of information and cyber security cost optimization

Kononovich Vladimir[1]

Sievserinov Oleksandr[2]

Romanyukov Mykola[3]

[1]Odessa National Polytechnic University, 65044, Ukraine, Odessa,
Shevchenko Ave. 1, kononovich@ukr.net

[2]Kharkiv National University of Radio Electronics, 61166, Ukraine,
Kharkiv, Nauky Ave 14, oleksand.sievierinov@nure.ua

[3]Kharkiv National University of Radio Electronics, 61166, Ukraine,
Kharkiv, Nauky Ave. 14, nikolay.romanyukov@gmail.com

Abstract. *The growing vulnerability of each individual in a progressive information and communication society is undeniable. Thus, on the part of the state, as well as the owner of the information to be protected, it is necessary to create new mechanisms that meet the modern requirements of individual protection of each subject of the system in information and cyberspace. This paper presents an effective method for calculating information and cybersecurity cost optimization. The class of societal attacks, which are identified as the most dangerous ones, is considered.*

Keywords: *information and cybersecurity; cost optimization; social engineering.*

I. Introduction and Problem statement

The significant development of progressive information technologies, combined with the communicative capabilities of the global digital "world", creates a number of grounds for regulating the security of these processes at the national and global level. The state information policy of Ukraine calls for new approaches to address information and cybersecurity issues, which is today the main component of national security and defense of the state [1].

The growing vulnerability of each individual in a progressive information and communication society is undeniable. Thus, on the part of the state, as well as the owner of the information to be protected, it is necessary to create new mechanisms that meet the modern requirements of individual protection of each subject of the system in information and cyberspace.

To date, the question of choosing the optimality criterion, taking into account the most dangerous class of attacks and a pessimistic strategy in modeling the process of optimization of information and cybersecurity costs, remains unresolved. Also, expert judgment is not taken into account when carrying out an information operation in terms of a measure of uncertainty that contains uncertainty.

The purpose of the work is to develop a method for optimizing information and cybersecurity costs. Identify the most dangerous class of information and cyber security attacks. Using subjective logic theory to account for uncertainty in estimates of possible costs by information and cybersecurity experts.

II. Problem solution and Results

Formulation of the problem. To date, the question of choosing the optimality criterion, taking into account the most dangerous class of attacks and a pessimistic strategy in modeling the process of optimization of information and cybersecurity costs, remains unresolved. Also, expert judgment is not taken into account when carrying out an information operation in terms of a measure of uncertainty that contains uncertainty. Currently, there are several criteria for modeling the information operation process for the best possible pessimistic strategy: Laplace, Valda, Hurwitz, Bayes-Laplace and Sevid [2]. Using the priority of the choice of the decision in the absence of sufficiently complete information about the state of the system, in order to prevent excessively large losses, which can lead to the wrong decision, the criterion of the optimality of Sevid was chosen, which fully meets the requirements [3]. Using Sevid's optimality criterion, we propose a specific algorithm to solve the problem of information and cyber security minimization and introduce the following values: for the protection side, the Boolean variable $x_j \in \{0,\ 1\}\ \forall_j \in M$ where $M = \{1,2..m\}$ multiple indices of remedies; $x_j = 1$ if $j-s$ protection will be used to protect against potential threats; $x_j = 0$ if $j-s$ no remedy will apply. Then $\vec{X}$ - the vector of boolean variables x_j ;for the attack side, the boolean variable $x_i \in \{0,\ 1\}\ \forall_j \in N$ where $N = \{1,2..n\}$ – set of indices of means of attack; $y_i = 1$, if the party to the attack applies $i-s$ a means of attack; $y_i = 0$ if the attack is not applied $i-s$ a means of attack. Then $\vec{Y}$ – vector Boolean variables $y_i\ .V_{\max}(y)$ – the maximum possible damage from the implementation of attacks without the use of remedies for the defense party; $V_{biasted}(X,Y)$ – damages to the defense party in the event of a biased application of its protective equipment; V_I – average losses from impartiality $i-s$ threats; P_{ij} - probability to prevent $i-s$ the threat from the attack.

The essence of the algorithm is to solve the problem with Boolean programming, so a guaranteed result is achieved in terms of damage from attacks by defense. The algorithm that allows solving problems in Boolean programming corresponds to the method of implicit search on a vector lattice by the rule "1 dominates 0" [2]. Maximum cost optimization by a given criterion is achieved by introducing the following restrictions, when real losses for the protection side can be represented in the form [2]:

$$\begin{aligned} V(\vec{X},\vec{Y}) &= V_{\max}(\vec{Y}) - V_{ynep}(\vec{X},\vec{Y}) = \\ &= \sum\nolimits_{i\in N} v_i y_i - \sum\nolimits_{i\in N} v_i y_i \max\nolimits_{j\in M} \{P_{ij}, x_j\} \end{aligned}, \qquad (1)$$

The defense side tries to minimize these losses and maximizes the attack side, meaning we have a zero sum game.

Since the choice of remedies solves the problem of minimizing the potential damage from attacks by the attacker, the Sevid criterion is transformed into a minimum risk criterion:

$$\begin{gathered}\min{}_{X\in\Delta x} \to admiss.\max{}_{Y\in\Delta y} \to admiss. \\ [\max{}_{X\in} \to admiss.\forall(\vec{X},Y)-V(\vec{X},\vec{Y})]\end{gathered}, \qquad (2)$$

The given formulation of the mathematical model of antagonistic play is considered in a separate example. Given that more than 70 percent of all information security breaches are due to the “human factor”, social engineering capabilities are widely used to obtain information about the attack object needed to provide NMS to the cybersecurity system. The main threats of social engineering from undesirable leakage of information according to statistics from [4], possible losses for the period of eight months and the conditional costs of the male-male attackers to carry out appropriate attacks during this period, are given in Table. 1.

Table 1. Losses from socio-technical attacks and the cost of their implementation

№	Threats	Damage from unbiased actions, thousand UAH	Cost of realization of threat of attacker, thousand UAH
1	Email	600	120
2	Telephone connection	300	60
3	Trash analysis	50	12
4	Personal approach	40	10
5	Reversing social engineering	140	16

IV.

Email threats are effective in spreading phishing messages with destructive information content. Damage data depend to a large extent on the specific activity of the attacked object and is therefore arbitrary given that, in the case of unbiased defense actions, the costs of the defenders' side significantly exceed the costs of the attacker's side [2].

Table 2 shows the methods of protection against threats, which are given by their numbers in accordance with table. 1, the cost of their implementation and the likelihood of threat prevention in the span of eight months.

Table 2. Methods for protection against security threats, the cost of their implementation and the likelihood of preventing threats in the span of eight months

№	Methods of protection	Cost of implementation, thousand UAH.	Probability of threat prevention				
			Threat numbers (Table 1)				
			1	2	3	4	5
1	Legislative	20	0,1	0,1	0,2	0,5	0,1
2	Morally ethical	27	0,6	0,5	0,2	0,3	0,4
3	Organizational and administrative	20	0,7	0,6	0,0	0,0	0,3
4	Organizational and technical	17	0,6	0,5	0,1	0,0	0,3
5	Informational	25	0,7	0,6	0,4	0,3	0,4
6	Organizational and economic	30	0,1	0,1	0,5	0,4	0,1
7	Engineering and technical	32	0,1	0,1	0,5	0,2	0,1

The approximate prices are given in Table. 2 define the security system configuration for the information system, taking into account their functional features [2]. Taking into account the initial data table. 1 and 2, and using the Boolean programming algorithm, we obtain solutions for the security side $\vec{X}=\|0,1,1,1,1,0,0\|$ and for the attack side $\vec{Y}=\|1,1,0,0,1\|$. This means that the selected methods of protection by the numbers 2,3,4,5 from the table. 2 and attack methods 1,2,5 from table. 1. The solution of the problem is optimal for the defense side, as in the case of biased defense action it is possible to reduce by 2.2 times the expenses (89 thousand UAH) compared to the expenses of the attacker (196 thousand UAH) and with high probability to eliminate all possible threats to social engineering. Analysis shows that email is the most vulnerable to the user.

For greater visibility of the obtained results, we will plot graphically the protection costs in the case of impartiality $P_{i.c}$ and prejudices $P_{p.c}$ measures according to the attacker's expenses $P_{a.}$ .For convenience, we plot graphs in the coordinate system of decimal logarithms $\lg(P_{i.c};P_{p.c.})$ and $\lg P_{a.}$ and are presented in Fig. 1.

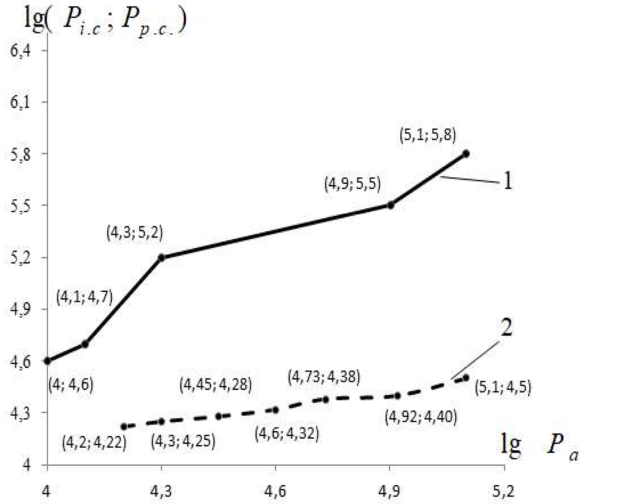

Figure 1. Loss dependency graphs $P_{i.c}, P_{p.c.}$ from social attacks $P_{a.}$: 1 – case of impartiality $P_{i.c}$ 2 – prejudices $P_{p.c}$

Graph 1 shows a significant increase in costs $P_{i.c}$ in the case of unbiased actions of the defender when the cost of the attacker increases $P_{a.}$. Graph 2 shows a significant reduction in costs $P_{p.c.}$ in the case of a biased application by the party of protection of the appropriate methods of protection (by numbers 1 - 7) according to the expenses in the unbiased actions of the defender $P_{i.c}$. Graphical dependence 2 corresponds to the optimal choice of methods of protection against social attacks.

For the right choice of optimal methods of protecting information with minimal cost, it is important to have a preliminary expert assessment of the possible risks in the conditions of certain uncertainty. Using Sevid's criterion, we construct a "risk matrix" for the above problem in order to make a decision that provides the minimum maximum risk value:

$$M=\left|\begin{array}{cc||c|} & & \max r_{ij}\\ 600 & 10 & 600\\ 300 & 12 & 300\\ 140 & 16 & 140\\ 120 & 40 & 120\\ 60 & 50 & 60^{*}\end{array}\right., \tag{3}$$

To the right of the "risk matrix" is the maximum risk column for each strategy A_i. Risk minimization is achieved when choosing a strategy A_5: 60 thousand UAH e-mail attacks.

The assessment of potential threats by information and cybersecurity professionals causes some uncertainty or uncertainty. The subjective logic theory (SL), developed by the Norwegian scientist A. Josang (Audum Jodsng), serves as an analytical description of such situations [5]. The centrality of subjective logic is the operation of three parameters. These parameters characterize the degree of trust (b), distrust (d), and uncertainty (u), provided that the true statement is arbitrary. The ability of SL theory to account for the uncertainty in the estimation of the possible costs by the defender, the possibility of interpreting its parameters, the presence of operators evaluating experts, makes it expedient to use it as an analytical apparatus. In this case, uncertainty is seen as filling the “vacuum” between trust and distrust. This situation can be mathematically expressed by the relation [5]:

$$\begin{array}{l} b+d+u=1;\\ \{b,d,u\}\in[0,1] \end{array}, \tag{4}$$

One of the common tasks for information and cybersecurity is to determine the security of security features. To calculate a generalized opinion about the reliability of security remedies, it is necessary to use operators, the result of which is an opinion that confirms:

a) the belief in the simultaneous truth of the assertions concerning the reliability of all elements of protection;

b) the belief that one or more of the assertions regarding the reliability of the security features are true.

The following requirements are met by operators:

a) conjunctions of assertions;

b) the disjunction of assertions.

According to current views on information and cybersecurity, information and cyber security risk analysis is an integral part of information and cyber security activities.

At risk we will understand the product of the probability of carrying out the risk and the cash equivalent of the loss from the side of protection from its realization

To calculate subjective likelihood of risk, we use the statement conjunction operator, which is equivalent to the product of the likelihood of statements, if the opinions are dogmatic. The result of a conjunction operation is an opinion that is calculated on the basis of opinion W_X^A and W_Y some expert judgment A on the truth of the two statements X and Y and signifies a simultaneous belief in the truth of both statements.

The method of optimizing information and cybersecurity costs consists of the above advanced algorithm, as well as taking into account elements of subjective logic theory. In addition, subjective logic operates with a vector of thoughts that can be represented as a vector $W_p=\{b_p,d_p,u_p,a_p\}$. Vectors of thought are considered individually and necessarily belong to someone and belong to something. subjective logic operators are used to calculate the vectors of thought corresponding to expert judgment.

III. Conclusions

The method of optimization of information and cybersecurity costs is presented. The example of consideration of the attacker's socio-technical attacks shows the results of the defense party's cost calculations in the case of unbiased and biased actions. The use of Sevid's optimality criterion allows to set the minimum and maximum risks of monetary protection costs. E-mail has been shown to be the most vulnerable element in socio-technical attacks. Since in most cases, the interaction between the defense and the assault side takes place under uncertainty, expert attention is based on the theory based on subjective logic.

References

[1] Stepanov V.Yu. Information security as a component of state information policy / V.Yu. Stepanov [Electronic resource] // State building. - № 2, - Kharkiv, 2016. - P. 525-542. - Access mode: http://www.kbuapa.kharkov.ua/e-book/db/2016-2/doc/1/02.pdf.J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] Bykov A.Yu. The task of choosing information protection tools in automated systems based on the antagonistic game model /A.Yu. Bykov, N.O. Altukhov, A.S. Sosenko. // Engineering Herald. - 2014. - No. 4. - S. 525–542.

[3] Abdenov A.Zh. The choice of means of effective protection using the methods of game theory / A.Zh. Abdenov, R.N. Zarkumova // Issues of information security. - 2010. - No. 2. - S. 26-31.

[4] Buryachok VL Information and cyber security: the social aspect: a textbook / [VL. Buryachok, VB Tolubko, V.O. Khoroshko, S.V. Tolupa]; for the total. ed. Dr. Techn. of Sciences, Professor VB Crowd. - K .: DUT, 2015. - 288 p.

[5] A. JosangAn Algebra for Assessing Trust in Certification Chains. InJ. Kochmar, editor, Proceedings of the Network and distributed Systems Security Symposium (NDSS’99). The Internet Society, 1999.

[6] Simonov S., Technologies and tools for risk management // Newsletter Jetinfo No. 2 (117), 2003. - S. 1-32.