Розглядаються проблема багатокритеріального аналізу ефективності консервативних систем захисту інформації, структура та складові яких не змінюються протягом деякого часу. Структурна схема таких систем включає об'єкт захисту, вразливості – канали для атак, загрози та засоби захисту.

За припущення про незалежність атак та засобів захисту розвинуто дискретну ймовірнісну модель ушкодженості об'єкта захисту. Для випадкової величини кількості ушкоджень за фіксований проміжок часу отримано представлення у вигляді суми біноміально розподілених випадкових величин, які залежать від параметрів атак та захисту. Подібно описано випадкові величини економічних втрат, часу відновлення та затрат на відновлення, для яких знайдено в аналітичному вигляді математичні сподівання та дисперсії. Для забезпечення високої статистичної надійності показники ризику запропоновано визначати за допомогою нерівності Кантеллі. На цій основі сформульовано ряд показників ефективності системи захисту, які характеризують ймовірність неушкодженості об'єкта захисту, залишкові втрати, умовно збережені кошти, живучість та затрати на відновлення.

З використанням теорії оптимальності за Парето розроблено методику багатокритеріального аналізу та раціонального проектування консервативних систем захисту інформації. Апробацію проведено для систем захисту аудіо інформації. Фронт Парето досліджено за критеріями економічної вигоди та інвестиційних затрат для 66 варіантів захисту. Вивчено вплив рівня захисту на показник Кантеллі умовно збережених коштів та вклад у нього засобів захисту різного типу.

Результати досліджень підтвердили закон насичення Гордона-Льоба, коли надмірний захист не приводить до підвищення ефективності систем захисту

Ключові слова: системи захисту інформації, ризик, ефективність, багатокритеріальний аналіз, модель Гордона-Льоба

UDC 004.681
DOI: 10.15587/1729-4061.2019.166349

A MULTICRITERIAL ANALYSIS OF THE EFFICIENCY OF CONSERVATIVE INFORMATION SECURITY SYSTEMS

V. Dudykevych
Doctor of Technical Sciences, Professor*
I. Prokopyshyn
PhD, Associate Professor
Department of Mathematical Modeling
Ivan Franko National University of Lviv
Universitetska str., 1, Lviv, Ukraine, 79000
E-mail: lviv.pi@gmail.com
V. Chekurin
Doctor of Physical and Mathematical Sciences, Professor
Department for Mathematical Problems
of Mechanics of Heterogeneous Solids
Pidstryhach Institute for Applied Problems of Mechanics and
Mathematics of the National Academy of Sciences of Ukraine
Naukova str., 3-b, Lviv, Ukraine, 79060
Technical Department
Kujawy and Pomorze University in Bydgoszcz
Torunska str., 55-57, Bydgoszcz, Poland, 85-023
I. Opirskyy
Doctor of Technical Sciences*
Yu. Lakh
PhD*
T. Kret
Assistant*
Ye. Ivanchenko
PhD, Associate Professor**
I. Ivanchenko
PhD**
*Department of Information Security
Lviv Polytechnic National University
S. Bandery str., 12, Lviv, Ukraine, 79013
**Department of Information Technology Security
National Aviation University
Kosmonavta Komarova ave., 1, Kyiv, Ukraine, 03058

1. Introduction

The three main resources used by humans in their life activities are information, matter, and energy. The task on information security is gaining increasingly greater importance due to the wide application of information technology in all spheres, as well as its affordability. Unauthorized interference in the information flows among computerized systems can

lead both to local problems and global threats to the technological, economic, political, and military security, as well as the safety of a state in general.

Based on the results from annual experts' business risk analysis «Allianz Risk Barometer» that has since 2001 been compiled by the financial group Allianz Global Corporate & Specialty, cyber-risks shifted from position 15 in 2013 to position 2 in 2018 [1]. The report by the World Economic Forum «Regional risks for business 2018» [2] identified cybersecurity as the main risk for Europe, Asia-Pacific and the Americas.

Therefore, it is a relevant issue to assess risk and overall effectiveness of information security systems.

2. Literature review and problem statement

Assessment of the effectiveness of security systems is a complex and multifaceted task, predetermined by the structural complexity of information systems and, accordingly, security systems, by the variety of vulnerabilities and the non-regular character of threats.

The effectiveness of protection systems is defined, above all, by their capability to reduce risks, which is why indicators for residual risks are among the main indicators for the efficiency of these systems.

A series of methods were developed in order to quantitatively describe risks, which employed both classic stochastic models [3, 4] and the theory of fuzzy sets [5, 6], and the game theory and simulation modeling [4, 7, 8].

When using stochastic models, the widely applied risk indicator is the mathematical expectation for a random variable (r. v.) of possible losses over a year – Annual Loss Expectancy (ALE) [3, 4]. In this case, scientists often scale the probabilities and possible consequences of threats, followed by the construction of matrices of expected losses for all threats, and a summary matrix of losses for which a numeric or symbolic scale for the magnitude of a risk is introduced. Based on the overall magnitude of ALE, they calculate relative indicators, accepting as a base the cost of capital, invested funds, possible losses if not protected, etc.

A general economic model for the dependence of mathematical expectation of conditionally saved funds on the magnitude of investment in information security, the expected net benefits from an investment in information security (ENBIS), was proposed in paper [9]. This model underlies a series of works whose results are generalized in study [10].

Although the mathematical expectation of losses satisfies all axioms of coherence on risk measures [11], for a symmetrical distribution of losses, this magnitude can be exceeded with a probability of 50 %. Therefore, it is suitable for the case when the standard deviation of losses is small.

For a more accurate description of risk, researchers apply, in particular, a quantile of a certain level in the distribution function of a random variable of losses – Value at Risk (VaR), or the mathematical expectation of losses that exceed this magnitude – Conditional Value at Risk (CVaR) [12]. The application of these risk measures for the assessment of informational risks was considered in papers [13–16]. Specifically, work [13] investigated the dependence of indicator VaR for the losses of information security on average daily cost of protection based on the simulation of loss of data for a group of financial companies, without considering the structure of protection. A model and an algorithm for calculating the magnitude of VaR of losses for cybersecurity systems based on the dynamic Bayesian networks to simulate the attacks and on the Monte Carlo method were proposed in paper [14]. A modeling problem on the calculation of loss indicators VaR and CVaR for a corporate information system, based on an empirical distribution function, was considered in [15]. A problem on the bicriterial optimization for the criteria cost-risk using the VaR and CVaR risk measures was investigated in paper [16].

The calculation of VaR and CVaR risk indicators requires the knowledge of an empirical distribution function of a random magnitude of losses, or the approximation of the upper tail of its distribution function with known distribution [12]. A risk measure that is close to VaR, yet a simpler one, is derived from the Chebyshev-Cantelli inequality [17]; the Chebyshev inequality was used in paper [18] to assess risk for a system of information security.

In addition to the indicators for residual risk, also of importance for information security systems are the average time of system recovery, average costs of recovery, probabilities of damage to a protected object, capital and current costs, etc.

Therefore, in general, assessing the effectiveness of information security systems is multicriterial in character.

The issue on a multicriterial analysis of efficiency of information security systems has not been studied in detail. Paper [7] reports a comparative analysis of eight studies in this field up to 2016, which applied the apparatus of a game theory and combinatorial optimization.

Paper [19] proposes a procedure for a multicriterial estimation of cybersecurity risks and the effectiveness of countermeasures based on the method of scalarization and expert assessments. The total risk estimate is obtained as a linear combination of the individual risk indicators, which, in turn, may be represented similarly through the lower-level risk indicators. Similarly defined are the efficiency indicators for countermeasures in terms of respective risk taking into consideration the magnitude of the latter. The total efficiency indicator equals a linear combination with some of the weight coefficients for certain lower-level performance indicators. In addition to expert estimates for individual risks and countermeasures, the procedure requires expert assessment of weight coefficients in the method of scalarization. The authors considered a model example of ranking five cybersecurity strategies based on effectiveness.

Study [20] addresses the task on choosing an optimal plan to protect an information-telecommunication system based on the criteria of the largest financial attractiveness and the lowest indicator of the overall impact on a business-process (operational impact assessment – OIA). The focus is on assessing the OIA indicator, which is defined by the authors as the probability of a conflict with a company's mission and is calculated based on the authentic procedure.

Our analysis testifies to the expediency of devising a procedure for a multicriterial estimation of the effectiveness of information security systems by using an adequate and simple model of damage caused by attacks, which would take into consideration the structure of protection, as well as the stochastic character of threats' effect.

3. The aim and objectives of the study

The aim of this study is to devise and verify a procedure for a multicriterial analysis of the efficiency of conservative information security systems based on a discrete probabilistic model of losses caused by attacks. That would make it possible

to perform a comparative analysis of the effectiveness of protection variants when designing security systems and to examine the contribution of different protection tools to security.

To accomplish the aim, the following tasks have been set:

– to advance a discrete probabilistic model of security system that takes into consideration the structure of protection and the random character of threats and provides an analytical description for the random variable of losses caused by attacks;

– to define simple and reliable indicators for residual risk based on the Cantelli inequality, as well as other indicators for the effectiveness of a security system;

– to apply a Pareto optimality theory to devise a procedure for a multicriterial analysis of the security system efficiency;

– to perform practical verification of the procedure for a multicriterial analysis of efficiency for the audio information security systems.

4. Development of a discrete probabilistic model of losses considering the structure of protection

The systems of technical protection are complex technical systems that enhance the safety of protected objects against illegal acts and other influences that may disrupt their functioning. The concept of a technical protection system covers the following basic components: protected objects, vulnerabilities, threats, protection tools, as well as a security management system. For conservative or static security systems whose structure and components do not change over a long time, the security management system is used only to control protection tools and replace them in case of malfunctioning.

Such a simplified scheme (object, vulnerabilities, threats, protection) makes it possible to describe in the same manner the systems of technical protection of different types, as well as combined systems, specifically information security systems. Authors of [18, 21] constructed a stochastic model of losses for it, as well as the procedure for estimating the economic efficiency of investment in security systems.

By following the methodology of these works in general, we shall consider a stochastic model with an investment horizon of one year, in which individual protected objects are aggregated into a single generalized object.

Assume the protected object O has K primary vulnerabilities $V^1, V^2, ..., V^K$, which are the channels for attacks. A security system includes M protection tools $S^1, S^2, ..., S^M$. Arrows in Fig. 1 show possible attacks of a primary damage, rectangles show the protection tools.

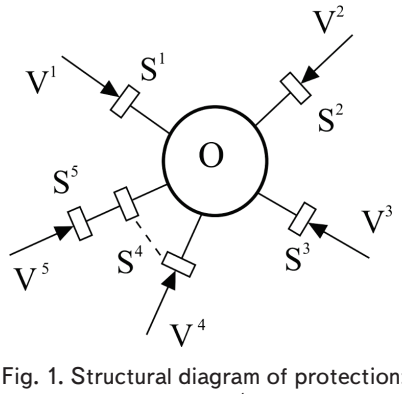

Fig. 1. Structural diagram of protection: O – protected object, V^k – vulnerabilities, S^m – protection tools

Assume that all attacks and protection tools are independent in the sense that the response by a protection tool to any attack is not related to other tools or attacks; all protection tools operate properly during an attack. We also believe that one knows the number of attacks along each channel over a year.

The probabilities of security breach S^m while protecting the V^k channel shall be denoted via a_{mk}, $m=1, 2, ..., M$, $k=1, 2, ..., K$. For the case when protection S^m does not protect the V^k channel, $a_{mk}=1$. Note that there is no need for the graphical representation of a security system since matrix $A=[a_{mk}]$ fully defines the structure of protection.

The probability of security breach along the V^k channel is equal to the product of probabilities of hacking all protection tools that protect this channel:

$$r_k=\prod_{m=1}^{M} a_{mk}. \quad (1)$$

Under the accepted assumption on the independence of protection tools and attacks, the total quantity of primary damage to the system will be the sum of binomially distributed random variables [21]:

$$\xi \sim \sum_{k=1}^{K} Bin\,(n_k, r_k), \quad (2)$$

where n_k is the average number of attacks per period along channel k, $Bin(n, r)$ is the binomially distributed r. v. with parameters n and r [17].

Note that for the case when the number of attacks n_k along channel k is less than unity, but one knows the probability of attack p_k, then one should put in formula (2):

$$n_k=1, \quad r_k=p_k\prod_{m=1}^{M} a_{mk}. \quad (3)$$

The absolute reliability of a security system is characterized by a probability of absence of any damage, which is equal to:

$$Q(\xi)=P\{\xi=0\}=\prod_{k=1}^{K}(1-r_k)^{n_k}. \quad (4)$$

The magnitude of total economic losses from a successful initial attack along channel V^k, taking into consideration secondary damage, shall be denoted via w_k. Assume that the losses from a possible damage to protection tools are negligible. Then the random variable of the total economic losses caused by attacks, considering formula (2), will be equal to:

$$\tilde{W}=\sum_{k=1}^{K} w_k Bin(n_k, r_k). \quad (5)$$

Based on it, we find the mathematical expectation for possible losses caused by attacks W_E, their variance W_D, as well as losses in the absence of protection tools W_*:

$$W_E=E(\tilde{W})=\sum_{k=1}^{K} w_k r_k n_k, \quad (6)$$

$$W_D=D(\tilde{W})=\sum_{k=1}^{K} w_k^2 r_k(1-r_k)n_k, \quad W_\sigma=\left(W_D\right)^{1/2}, \quad (7)$$

$$W_*=\sum_{k=1}^{K} w_k n_k. \quad (8)$$

Thus, in the framework of the proposed model, we have derived simple formulae for the probability of no damage to a protected object, the mathematical expectation, and the variance of losses caused by attacks.

5. Defining effectiveness indicators for a security system

The indicators for a random variable of losses caused by attacks do not include the cost of protection tools. Assume that the amount of current expenditures and the averaged capital cost of a protection tool S^m over a period is the magnitude C_m, then the total cost of equipment over a period equals:

$$C = \sum_{m=1}^{M} C_m. \tag{9}$$

Therefore, the random variable of total losses $\tilde{L}$ considering the costs and equipment will be equal to the sum of magnitudes (5) and (9):

$$\tilde{L} = C + \tilde{W}. \tag{10}$$

Its mathematical expectation and variance are determined as follows:

$$L_E = E(\tilde{L}) = C + W_E = C + \sum_{k=1}^{K} w_k r_k n_k, \tag{11}$$

$$L_D = D(\tilde{L}) = W_D = \sum_{k=1}^{K} w_k^2 r_k (1 - r_k) n_k, \quad L_\sigma = \left(L_D\right)^{1/2}. \tag{12}$$

Under assumptions $L_E < +\infty$, $L_D < +\infty$, as it follows from the Cantelli inequality [17], the total losses $\tilde{L}$ do not exceed the magnitude:

$$L_R = L_E + \lambda L_\sigma, \quad \lambda > 0, \tag{13}$$

at reliability:

$$\alpha = \lambda^2 / (1 + \lambda^2). \tag{14}$$

The random variable of conditionally saved funds is:

$$\tilde{B} = W_* - \tilde{L} = W_* - C - \tilde{W}, \tag{15}$$

at reliability α, it will be no less than magnitude:

$$B_R = W_* - L_E - \lambda L_\sigma. \tag{16}$$

The best variant is the protection with a lower indicator L_R, or with a larger indicator B_R.

Note that the magnitude of mathematical expectation for conditionally saved funds $B_E = W_* - L_E$ corresponds to the indicator ENBIS (expected net benefits from an investment in information security), introduced in paper [9].

To represent the results, it is also convenient to consider the dimensionless parameters. We shall introduce a dimensionless magnitude for conditionally saved funds $\tilde{b}$:

$$\tilde{b} = \tilde{B} / W_*. \tag{17}$$

Based on the formulae above, it is easy to write down the mathematical expectation and a standard deviation of this magnitude, denoted, respectively, by b_E and b_σ:

$$b_E = B_E / W_*, \tag{18}$$

$$b_\sigma = B_\sigma / W_*. \tag{19}$$

Similarly, at probability (18), the random variable $\tilde{b}$ will be no less than magnitude:

$$b_R = b_E - \lambda b_\sigma. \tag{20}$$

To describe the averaged cost of equipment, we shall also introduce a dimensionless indicator:

$$c = C / W_*. \tag{21}$$

Hereafter, the magnitude b_E is referred to as a mathematical expectation, or the average conditional saving, and the magnitude b_R – a Cantelli's measure of conditional savings.

We shall also record the r. v. of system recovery time $\tilde{T}$, which characterizes its survivability. To this end, we introduce the magnitude t_k for the total time of recovery after a successful primary attack along channel V^k, taking into consideration secondary damage.

Additionally, we assume that attacks do not occur while the system recovers. Then the r. v. of recovery time is recorded similar to (5):

$$\tilde{T} = \sum_{j=k}^{K} t_k Bin(r_k, n_k). \tag{22}$$

Its mathematical expectation, variance, and recovery time in the absence of protection tools are recorded similar to formulae (6) to (8):

$$T_E = E(\tilde{T}) = \sum_{k=1}^{K} t_k r_k n_k, \tag{23}$$

$$T_D = D(\tilde{T}) = \sum_{k=1}^{K} t_k^2 r_k (1 - r_k) n_k, \quad T_\sigma = \left(T_D\right)^{1/2}, \tag{24}$$

$$T_* = \sum_{k=1}^{K} t_k n_k. \tag{25}$$

Similarly, one can determine a random amount of funds for recovery. This magnitude does not equal the total losses caused by attacks, since the latter include possible losses caused by information leak.

Note that for the r. v. of the system recovery time (22) and the cost of recovery it is easy to record indicators, similar to (18), (20).

Thus, for a conservative system of information security, under a series of simplifying assumptions on attacks and protection, we have defined a series of indicators, averaged over a period, which variously characterize a system of protection.

6. Procedure for a multicriterial assessment of security systems

Let $\mathbf{S} = (S^1, S^2, \ldots, S^M)$ be a set of protection tools (a protection variant), $\mathbf{f}(\mathbf{S}) = \left(f_1(\mathbf{S}), f_2(\mathbf{S}), \ldots, f_l(\mathbf{S})\right) \in \mathbf{R}^l$ – a vector of criteria, X is the set of permissible variants, $I = \{1, 2, \ldots, l\}$ is the set of indexes. One can then state the problem on a multicriterial optimization for choosing the optimal protection variant [22]:

$$\mathbf{f}(\mathbf{S}) \to \max_{\mathbf{S} \in X}. \tag{26}$$

To analyze this problem, we introduce the notion of dominance and effective set [22]. Protection $\mathbf{S}_1$ dominates over

protection $\mathbf{S}_2$ ($\mathbf{S}_1 \succ \mathbf{S}_2$) if it is not worse than $\mathbf{S}_2$ for all the criteria and is the best for at least one, that is the following condition is satisfied:

$$\left(\mathbf{f}(\mathbf{S}_1) \neq \mathbf{f}(\mathbf{S}_2)\right) \wedge \left(\mathbf{f}(\mathbf{S}_1) \geq \mathbf{f}(\mathbf{S}_2)\right). \quad (27)$$

An effective set $P(X) \subset X$ (a Pareto set) denotes the set of non-dominating protection variants – those options that are not dominated by any other variant from the permitted set:

$$P(X) = \{\mathbf{S}' \in X \mid \forall \mathbf{S} \in X \ \mathbf{f}(\mathbf{S}) \neq \mathbf{f}(\mathbf{S}') \Rightarrow$$
$$\Rightarrow \exists\, i \in I: \ f_i(\mathbf{S}) < f_i(\mathbf{S}')\}. \quad (28)$$

Vectors from the effective set cannot be improved for any criterion without compromising other criteria. That is why the points within this set are accepted as a compromise solution to the problem of a multicriterial optimization (26).

In our case, the permissible set is a finite discrete set. Therefore, it is possible to construct the effective set by consistent sorting of pairs excluding from further consideration the dominated variants based on definition (28). For a two-dimensional and a three-dimensional case, it is easy to represent an effective set graphically in the criteria space.

7. Results of studying the effectiveness of audio information security system

We have examined a one-year investment project of a system to protect business premises from audio information leakage. Calculations were carried out by means of electronic spreadsheets.

General characteristics for attacks and protection tools, the price of protection tools, were acquired from the Internet, numerical characteristics for attacks and the reliability of protection tools were derived from an expert analysis [23].

We considered 8 types of vulnerabilities that are described in Table 1.

Table 1

Description of vulnerabilities and attacks

Channel number	Channel title	Number of attacks, or the probability of an attack per a year	Magnitude of losses caused by a successful attack, UAH thousand
1	V_1 – radio microphones	10	40
2	V_2 – digital communication	16	40
3	V_3 – direct electromagnetic radiation and induction	20	40
4	V_4 – dictaphones	12	40
5	V_5 – construction structures	24	40
6	V_6 – electric grid	10	40
7	V_7 – burglar and fire alarm systems	10	40
8	V_8 – telephone line	10	40

We used 11 types of protection tools whose characteristics are given in Table 2. Trade names of the tools are not provided to prevent bad publicity.

Table 2

Characteristics of protection tools

Number of protection – m	Total cost, UAH thousand	Probability of security breach m during attack along channel k–a_{mk}							
		k=1	k=2	k=3	k=4	k=5	k=6	k=7	k=8
1. Wideband radio channel blockers									
1	19	0.08	1	0.10	1	1	1	1	1
2	16	0.05	1	0.05	1	1	1	1	1
3	15	0.10	1	0.10	1	1	1	1	1
4	10	0.10	1	0.10	1	1	1	1	1
2. Digital channels protection									
5	114	1	0.03	1	1	1	1	1	1
6	86	1	0.04	1	1	1	1	1	1
7	48	1	0.04	1	1	1	1	1	1
8	27	1	0.05	1	1	1	1	1	1
9	10	1	0.05	1	1	1	1	1	1
3. Systems of acoustic and vibroacoustic protection									
10	85	0.01	0.01	0.01	0.01	0.01	0.01	0.01	0.01
11	24	0.02	0.02	0.02	0.02	0.02	0.02	0.02	0.02
12	26	0.03	0.03	0.03	0.03	0.03	0.03	0.03	0.03
13	12	0.04	0.04	0.04	0.04	0.04	0.04	0.04	0.04
14	12	0.07	0.07	0.07	0.07	0.07	0.07	0.07	0.07
4. Vibroacoustic noise generators									
15	22	1	1	1	1	0.03	1	1	1
16	18	1	1	1	1	0.04	1	1	1
17	14	1	1	1	1	0.05	1	1	1
18	10	1	1	1	1	0.06	1	1	1
5. Dictaphone jammers									
19	124	1	1	1	0.01	1	1	1	1
20	37	1	1	1	0.02	1	1	1	1
21	19	1	1	1	0.03	1	1	1	1
22	8	1	1	1	0.05	1	1	1	1
6. Power supply filters									
23	17	1	1	1	1	1	0.02	1	1
24	15	1	1	1	1	1	0.02	1	1
25	13	1	1	1	1	1	0.03	1	1
26	9	1	1	1	1	1	0.03	1	1
7. Filters of burglar and fire alarm systems									
27	3	1	1	1	1	1	1	0.01	1
28	3	1	1	1	1	1	1	0.02	1
29	3	1	1	1	1	1	1	0.03	1
8. Telephone lines filters									
30	4	1	1	1	1	1	1	1	0.01
31	3	1	1	1	1	1	1	1	0.02
32	2	1	1	1	1	1	1	1	0.02
33	3	1	1	1	1	1	1	1	0.02
9. Scanning radio receivers									
34	170	0.02	0.03	0.03	1	1	1	1	1
35	35	0.03	0.04	0.05	1	1	1	1	1
36	28	0.03	0.04	0.05	1	1	1	1	1
37	12	0.04	0.05	0.1	1	1	1	1	1
38	10	0.04	0.05	0.1	1	1	1	1	1
10. Universal search tools									
39	401	0,01	0.01	0.02	1	1	0.01	0.01	0.01
40	291	0,01	0.01	0.02	1	1	0.01	0.01	0.02
41	279	0,02	0.03	0.03	1	1	0.01	0.01	0.02
42	225	0,03	0.03	0.03	1	1	0.02	0.02	0.02
43	110	0,03	0.03	0.03	1	1	0.02	0.02	0.02
11. Nonlinear locators									
44	602	0.02	0.02	1	0.02	1	1	1	1
45	393	0.02	0.02	1	0.02	1	1	1	1
46	236	0.03	0.03	1	0.03	1	1	1	1
47	199	0.03	0.03	1	0.04	1	1	1	1
48	182	0.04	0.04	1	0.04	1	1	1	1

We studied 66 variants of varying degrees of protection when some of the channels are unprotected, all channels are protected by a single or several protection tools. For risk indicators, we used a parameter value $\lambda=3$, which ensures their 90 % reliability ($\alpha=0.9$).

The results of analysis of the two-criterial optimization problem with a vector criterion $(-c(\mathbf{S}),\ b_E(\mathbf{S}))$ are shown in Fig. 2. Letters *A*, *B*, *C* mark the points from the effective set. A solid curve represents the mean square approximation of dependence $b_E \sim c$ using a Gordon-Loeb approximation [9]:

$$b_E \approx 1-(\alpha c+1)^{-\beta}-c, \qquad (29)$$

where $\alpha>0$, $\beta>0$ are the numeric parameters.

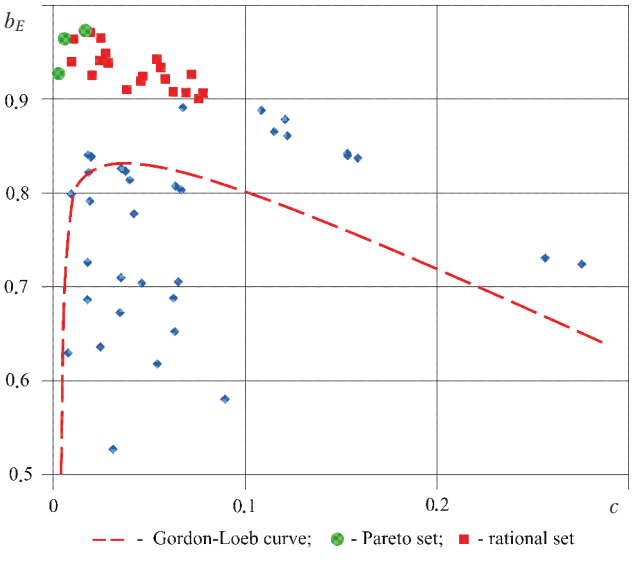

Fig. 2. Dependence of mathematical expectation for conditional saving b_E on the index of investment volume c

Point $A(0.0028;\ 0.9272)$ and point $B(0.0058;\ 0.9272)$ correspond to the protection variants with a single protection tool – $\mathbf{S}=(14)$ and $\mathbf{S}=(12)$, and point $C(0.0066;\ 0.9730)$ – to the variant with five protection tools – $\mathbf{S}=(12, 24, 28, 31, 36)$. In the upper-left corner, red color highlights a set of rational protection variants whose efficiency exceeds 90 % for criterion b_E, and whose price is less than 10 % of losses in the absence of protection.

A similar study was conducted based on criterion $(-c(\mathbf{S}),\ b_R(\mathbf{S}))$, the results are shown in Fig. 3.

The points from the effective set $A(0.0028;\ 0.8549)$, $B(0.0058;\ 0.9158)$, $C(0.0066;\ 0.9446)$ correspond to the same protection variants in the previous case. In the upper-left corner, red squares show the set of rational protection variants whose efficiency exceeds 90 % for criterion b_R, and whose price is less than 10 % of losses in the absence of protection.

A solid curve shows the root mean square approximation of dependence $b_R \sim c$ using a Gordon-Loeb approximation (29).

In both cases (Fig. 2, 3), one observes the effect of saturation [9], when the increased investment in protection does not lead to the improvement of risk indicators.

An analysis of the standard deviation indicator b_σ has revealed that it does not exceed 3 % and decreases with an increase in the indicator of investment *c*. That is why the indicators of risk b_R (20) and mathematical expectation b_E (18) for the conditionally saved funds differ by less than 10 %. However, the set of rational protection variants based on the criterion of risk is twice smaller than the same set based on the criterion of mathematical expectation.

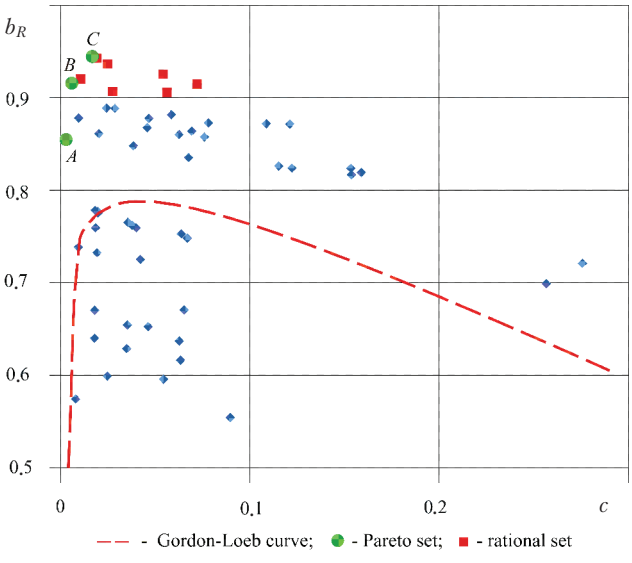

Fig. 3. Dependence of the Cantelli's measure of conditional saving b_R on the indicator of investment volume c

Denote the medium level of protection as the ratio of the number of protection tools to the number of vulnerabilities:

$$\mu = M / K. \qquad (30)$$

Fig. 4 shows the dependence of the Cantelli's measure of conditional saving b_R on the average level of protection μ. Similar to previous dependences, there is the saturation in terms of risk indicator if the average level of protection is greater than unity.

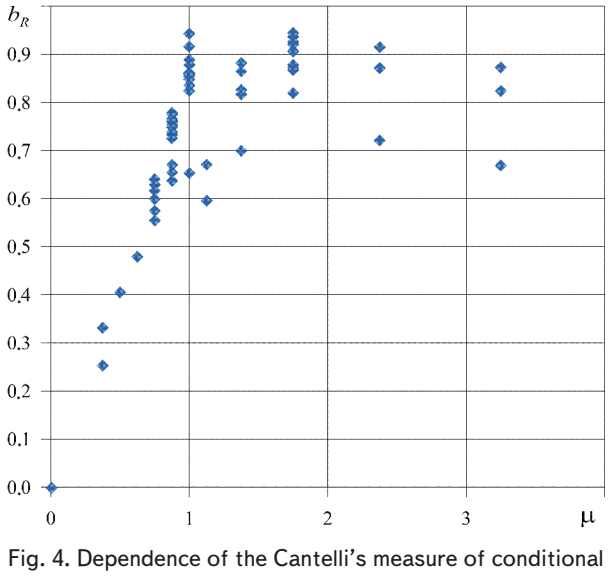

Fig. 4. Dependence of the Cantelli's measure of conditional saving b_R on the average protection level μ

Consider a protection variant $\mathbf{S}=(S^1, S^2,..., S^M)$. Let *H* be a certain measure of its efficiency, H_m – this indicator for the case when tool S^m is excluded from protection. The relative

contribution of protection tool S^m to indicator H is characterized by magnitude:

$$\delta_m = (H - H_m)/H, \quad m = 1, 2, ..., M. \tag{31}$$

We considered two similar protection variants whose protection tools belong to groups 1, 2, 4, 5, 6, 7, 8 (Table 2) but have a different price: $\mathbf{S}_1=(4, 7, 18, 22, 26, 29, 32)$ – cheaper, and $\mathbf{S}_2=(1, 5, 15, 19, 23, 27, 30)$ – expensive. Fig. 5 shows a comparative diagram of vectors $\delta=(\delta_1, \delta_2,..., \delta_7)$ for the specified variants.

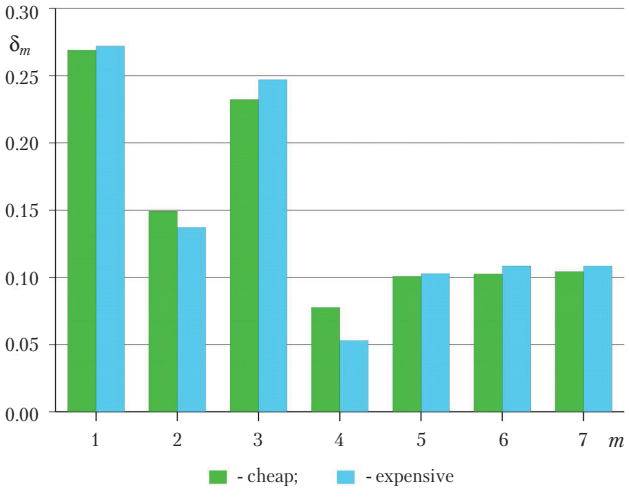

Fig. 5. Relative contribution of protection tools δ_m to the aggregate risk indicator b_R for various m: 1 – tools 4 and 1; 2 – 7 and 5; 3 – 18 and 15; 4 – 22 and 19; 5 – 26 and 23; 6 – 29 and 27; 7 – 32 and 30

We see that the greatest contribution to indicator b_R, regardless of cost, is provided by protection tools 1 and 3 (respectively, of type 1 and 4 from Table 2).

Similar studies can be performed for the other two or more criteria, specifically (4), (6), (7), (11) to (13), (18), (20), (21), (23), (24), (30).

8. Discussion of the results obtained; prospects for further research

We have developed a procedure for the multicriterial estimation of conservative security systems using a discrete probabilistic model of losses. Its advantages are simplicity and the application of risk indicators that are reliable in probabilistic sense, for which we have derived analytical formulae. In contrast to the general economic theories, our procedure takes into consideration the structure of protection and the stochastic nature of threats' effect. It reduces the task on assessing the effectiveness of a protection system to the estimation of separate protection tools and it makes it possible to solve a problem on the rational choice of protection variants. That makes it possible to calculate the mathematical expectation and indicators for the risk of losses caused by attacks, which is why it could be used to assess the cost of insurance rates when insuring security systems.

Of interest is the comparison of the obtained practical results with the economic theory by Gordon-Loeb [9], which confirmed the conclusion on that the over-protection could lead to a decrease in the overall efficiency of protection systems.

The shortcoming of the procedure is the assumption about a conservative (stationary) character of protection. However, one can apply it for a quasi-static analysis of dynamic security systems by assigning the required time of stationarity.

The procedure makes it possible to simultaneously consider the threats of a different nature, since it takes into consideration only their economic and probabilistic indicators. However, accounting for the interaction of threats is only possible through their aggregation into a single threat.

The proposed procedure for the multicriterial assessment of security systems is suitable for analysis of different types of security systems, specifically combined systems of information security and physical safety; it could be used in the development and testing of simulation models of protection systems. It allows the expansion towards considering multiple protected objects, describing the number of attacks as a discretely distributed random variable, reviewing investment projects of any duration.

The simplicity of the procedure makes it possible to use it in the learning process.

It is planned to further advance the proposed methodology for calculating insurance premiums when insuring security systems, simulation modeling of security systems, quasi-static analysis of dynamic protection systems.

9. Conclusions

1. We have advanced, for the conservative systems of information protection, a discrete probabilistic model that takes into consideration the structure of protection and provides an analytical notation of the random variable for the damage to a protected object. The model makes it possible to record simple formulae for the mathematical expectation and variance in a random variable of losses caused by attacks.

2. Based on the Cantelli's inequality, we have derived simple and statistically significant indicators for residual risks. The analytical form, which is convenient for practical use, has enabled the formulation of a series of known and new indicators for the effectiveness of information security systems that characterize the probability of damage to a protected object, conditional savings, time and costs of recovery.

3. In the framework of the model, based on the Pareto optimality theory, we have devised the procedure for a multicriterial analysis of protection systems efficiency. That makes it possible to perform the construction of an effective set of protection variants with a simple geometric interpretation for the case of two and three criteria.

4. 66 protection variants were investigated for the system that protects audio information. The effective set was built based on the criteria for the average conditional saving – investment costs, the Cantelli's measure of conditional savings – investment costs. In both cases, the effective set consists of three identical variants for protection, which demonstrate an investment cost indicator within 0.28–0.66 % of possible losses without protection.

We have also defined a set of rational protection variants whose efficiency exceeds 90 % for the criterion of economic

benefit, and investment costs are less than 10 % of losses in the absence of protection.

It was found that excessive protection leads to a decrease in the indicators for conditional savings, which agrees with the conclusions of the Gordon-Loeb economic model.

Our study has shown the simplicity and efficiency of the proposed procedure for a comparative analysis and rational selection of protection variants, for determining a contribution of various types of protection tools to performance indicators.

References

1. Allianz Risk Barometer: Top Business Risks for 2018. URL: https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2018.pdf
2. Regional Risks for Doing Business 2018: Insight Report. Geneva, 2018. 40 p. URL: http://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2018.pdf
3. Brotby W. K. Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement. Taylor & Francis, 2009. 200 p. doi: https://doi.org/10.1201/9781420052862
4. Sahinoglu M. Cyber-Risk Informatics: engineering evaluation with data science. Wiley & Sons, 2016. 560 p. doi: https://doi.org/10.1002/9781119087540
5. Korchenko O. H., Kazmirchuk S. V., Akhmetov B. B. Prykladni systemy otsiniuvannia ryzykiv informatsiynoi bezpeky. Kyiv, 2017. 435 p.
6. Yudin A., Buchyk S. Technology of construction and defence of the Ukrainian segment of the identifiers' tree of state informative resources on the basis of risk management // Zakhyst informatsiyi. 2016. Vol. 18, Issue 2. P. 107–114. URL: http://nbuv.gov.ua/UJRN/Zi_2016_18_2_5
7. Decision support approaches for cyber security investment / Fielder A., Panaousis E., Malacaria P., Hankin C., Smeraldi F. // Decision Support Systems. 2016. Vol. 86. P. 13–23. doi: https://doi.org/10.1016/j.dss.2016.02.012
8. Method for Optimization of Information Security Systems Behavior under Conditions of Influences / Hu Z., Khokhlachova Y., Sydorenk V., Opirskyy I. // International Journal of Intelligent Systems and Applications. 2017. Vol. 9, Issue 12. P. 46–58. doi: https://doi.org/10.5815/ijisa.2017.12.05
9. Gordon L. A., Loeb M. P. The economics of information security investment // ACM Transactions on Information and System Security. 2002. Vol. 5, Issue 4. P. 438–457. doi: https://doi.org/10.1145/581271.581274
10. Gordon L. A., Loeb M. P., Zhou L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model // Journal of Information Security. 2016. Vol. 07, Issue 02. P. 49–59. doi: https://doi.org/10.4236/jis.2016.72004
11. Coherent Measures of Risk / Artzner P., Delbaen F., Eber J.-M., Heath D. // Mathematical Finance. 1999. Vol. 9, Issue 3. P. 203–228. doi: https://doi.org/10.1111/1467-9965.00068
12. McNeil A. J., Frey R., Embrechts P. Quantitative Risk Management: Concepts, Techniques and Tool. Princeton and Oxford, 2005. 538 p.
13. Wang J., Chaudhury A., Rao H. R. Research Note – A Value-at-Risk Approach to Information Security Investment // Information Systems Research. 2008. Vol. 19, Issue 1. P. 106–120. doi: https://doi.org/10.1287/isre.1070.0143
14. CyberV@R. A Cyber Security Model for Value at Risk. Technical report / Raugas M., Ulrich J., Faux R., Finkelstein S., Cabot C. Baltimore MD, 2013. 45 p. URL: https://www.cyberpointllc.com/docs/CyberVaR.pdf
15. Dudykevych V. B., Lakh Yu. V., Prokopyshyn I. A. Otsinka vartosti ryzyku dlia system zakhystu informatsiyi // Informatsiyna bezpeka. 2011. Issue 1 (5). P. 44–49.
16. Sawik T. Selection of optimal countermeasure portfolio in IT security planning // Decision Support Systems. 2013. Vol. 55, Issue 1. P. 156–164. doi: https://doi.org/10.1016/j.dss.2013.01.001
17. Ross S. M. Probability models for computer science. Elsevier Science, 2002. 288 p.
18. Dudykevych V. B., Ivaniuk V. M., Prokopyshyn I. A. Efektyvnist investytsiy u systemy zakhystu prymishchen vid vytoku movnoi informatsiyi // Kompiuterni tekhnolohiyi drukarstva. 2014. Issue 32. P. 20–28. URL: http://nbuv.gov.ua/UJRN/Ktd_2014_32_4
19. Multicriteria Decision Framework for Cybersecurity Risk Assessment and Management / Ganin A. A., Quach P., Panwar M., Collier Z. A., Keisler J. M., Marchese D., Linkov I. // Risk Analysis. 2017. doi: https://doi.org/10.1111/risa.12891
20. Selection of Pareto-efficient response plans based on financial and operational assessments / Motzek A., Gonzalez-Granadillo G., Debar H., Garcia-Alfaro J., Möller R. // EURASIP Journal on Information Security. 2017. Vol. 2017, Issue 1. doi: https://doi.org/10.1186/s13635-017-0063-6
21. Dudykevych V. B., Prokopyshyn I. A., Chekurin V. F. Problems of efficiency estimation of security systems // Visnyk NU «Lvivska politekhnika». Avtomatyka, vymiriuvannia ta keruvannia. 2012. Issue 741. P. 118–122. URL: http://science.lpnu.ua/uk/node/3718
22. Ehrgott M. Multicriteria Optimization. Berlin Heidelberg, 2005. 323 p. doi: https://doi.org/10.1007/3-540-27659-9
23. Management of information protection based on the integrated implementation of decision support systems / Lakhno V., Kozlovskii V., Boiko Y., Mishchenko A., Opirskyy I. // Eastern-European Journal of Enterprise Technologies. 2017. Vol. 5, Issue 9 (89). P. 36–42. doi: https://doi.org/10.15587/1729-4061.2017.111081