UDC 004.056 DOI: 10.30748/soivt.2018.53.29

V. Shevchenko[1], D. Rabchun[2]

[1] *Taras Shevchenko National University of Kyiv, Kyiv*
[2] *State University of Telecommunications, Kyiv*

CHOICE AND JUSTIFICATION OF THE INTEGRAL INDEX AND CRITERIA OF THE EFFICIENCY LEVEL OF TARGET USE OF SOFTWARE INFORMATION SECURITY COMPLEX

Information security metrics are seen as an important factor in making sound decisions about various aspects of security, ranging from the design of security architectures and controls to the effectiveness and efficiency of security operations. The article is related to analysis of the indicators and criteria for assessing the efficiency of software information security complexes. In accordance with the requirements, authors proposes an integral indicator for evaluating the efficiency of the target use of software information security complexes in the conditions of dynamic information confrontation, which allows to use a dynamic approach to managing the resources of information systems security.

Keywords: security evaluating, security integral index, software information security, security metrics.

Introduction

Research objective and literature review. To assess the quality functioning of complex technical systems such as Software Information Security (SIS) Complex under different conditions and the influence of the external environment comparing among themselves we use indexes and criteria of quality and efficiency.

According to [1] indexes are quantitative characteristics of quality and efficiency, while criteria for evaluating the efficiency define conditions that must satisfy values of these indexes and indicate desirable level of system quality functioning and efficiency of carried out operations.

As the efficiency of SIS Complex [1] – is a operational feature of target-functioning system process, and the run-unit operation could distinguish itself from other processes by target objectives, consequently the index of efficiency should characterize the level of achieving the operation targets.

Therefore, targeting the accurate and correct operation formulation is thus essential for choosing the right index of efficiency.

There are a large number of research and regulatory documents aimed at measuring or evaluating security. Trusted Computer System Evaluation Criteria (TCSEC) [2], Information Technology Security Evaluation Criteria (ITSEC) [3], Systems Security Engineering Capability Maturity Model (SSE-CMM) [4], and Common Criteria [5]. Each of these works received only limited success. It is appropriate to conclude that the question of assessing the security of information systems is a rather complex issue, proceeding from the importance of the problem. Further evidence is that the topic, Security Metrics, was included in the latest hard problem list, prepared by INFOSEC Research Council.

The purpose of the work is to select the indicator and criteria for an adequate assessment of the efficiency of the SIS Complexes in the conditions of dynamic information confrontation.

Main material

Substantially the operation target can be defined differently, however in all cases it consists in obtaining necessary results.

Physically achievement of the operation target is an approach of some events, formally–it is a performance of some conditions under which the operation target can be considered as achieved.

It is also necessary to take into account the following features made in the course of the technical and special literature analysis [1], taking into consideration the results based on functioning of real complexes of SISC, it was determined that the choice of indexes efficiency level of target use of the specified systems along with the requirement of their coherence with objectives of operations:

- the chosen index of efficiency should objectively reflect the level of compliance of operation target and fully characterize it as uniform target process,
- the index of efficiency should consider a set of essential features of operation and reflect not only the general, but also special cases inherent in it;
- the index should be accurately focused on the end result of the application of system, the run-unit operation that is able estimate efficiency of the solution of the main objective of system, but not minor tasks;
- Besides, it is necessary that the chosen index of efficiency have such features:
- correct accounting of basic target of system and stochastic conditions of functioning;
- realizability (evaluation)

- unambiguity of quantitative expression of efficiency;
- stability;
- sensitivity to managing directors and the factors defining its value;
- usability and definitions without big expenses of resources and time;
- presentation and clear physical sense;
- constructability, flexibility and universality.

The achievement of an objective requires time spent and resources involved during target use of complex systems, such as SISC.

Therefore, the quality of target use can't be fully characterized by one of its operational features separately.

For a complex research of efficiency of each operation, the result index of quality should include three groups of the components, that are characterized by:

1) possible target effects (effectiveness of operation);

2) expenses of operational resources (resource intensity of operation);

3) time expenses (efficiency of operation).

For the formalized justified choice of an index of operation efficiency (target use of SISC) we will enter the following designations:

W – vector index of operation quality results;

$Y = (y_1 ... y_{n1})$ – vector of resources involved in obtaining results of operation;

$R = (r_1 ... r_{n2})$ – vector of operation results (target, positive effects);

$T = (t_1 ... t_{n3})$ – vector of time consumption to achieve target effects.

Then the index of operation quality results W is represented as a n-dimensional vector $n = n_1 + n_2 + n_3$:

$$W = (Y, R, T) = (Y_1 ... Y_{n1}; r_1 ... r_{n2}; t_1 ... t_{n3}).$$

By eliminating of indexes of partial effects, the n-dimensional vector can be reduced to a three-component vector. It can be received by introduction of the generalized indexes:

$$Y = \sum_{i=1}^{n_1} \alpha_i y_i ; \quad R = \sum_{j=1}^{n_2} \beta_i r_i ;$$

$$T = \max(t_1 ... t_{n3}),$$

where α, β – weighting coefficients.

After eliminating indexes of partial effects, the operation quality results will take a form:

$$W = (Y, R, T).$$

In the course of study, it was revealed that eliminating of partial indexes is correct only inside the group [6]. The criterion, estimates quality of operation, in this case can be presented by expression (1):

$$W \in \{W_D\}, \qquad (1)$$

where $\{W_D\} = (Y_D, R_D, T_D)$ – vector tolerance range, the vector of admissible value of operation resulting the target achievement, formally, it's implementation of condition (1).

Analysis of functioning of complex systems such as SISC [6] has demonstrated that the result of target use depends on the technical and economic characteristics and factors characterizing conditions while operating systems, that is

$$W = W(A', B'),$$

where A – vector of technical and economic characteristics of system;

B – vector of factors characterized by system operating conditions.

Accepted values W_D of vector W are defined by the conditions of system use, that is

$$W_D = W_D(B''),$$

where B'' – vector of factors, that is characterized by conditions of system use.

Conditions of functioning and target use of system in total, create conditions of carrying out operation which can be presented by a vector

$$B = B' \cup B''.$$

For complex systems such as SISC among components of vectors A, B' and B'' dominate stochastic features.

Coincidence of separate components of indicated vectors condition the stochastic character of vector W operation results, carried-out by SISC, and W_D vector tolerance range [7].

Thus, to fulfill a condition (1), means to achieve the target of operation that is a stochastic event therefore we can't judge operation efficiency, as the index of efficiency should characterize efficiency of operation integrally, but not it separate realization.

Therefore, as the index of operation efficiency should appear the probability of an event $W \in \{W_D\}$ – probability of achievement the operation target (probability of performance of SISC target task):

$$P_{DM} = p(W \in \{W_D\}) \; P_{DM} = p(W \in \{W_D\}).$$

Probability P_{DM} – characterizes degree of compliance of operation results W (its target and side effects) according to specified requirements.

This probability is the informative complex efficiency index of SISC target use as it not only characterizes the operation taking into account a correlation between target and side effects, but also establishes degree of operation target achievement [8].

According to the partition between opportunities of the SIS complex and realized results on target and

providing features, the N-dimensional vector of private indicators of operation results W can be presented in the form of two components: vector W_C of target operation indicators and vector W_Z providing (technical and economic) characteristics of SISC and target process of functioning.

Among the most significant technical and economic characteristics of SISC can be considered the following: availability (existence of the corresponding SIS) for effective functioning in the situation and stability [9].

Accordingly, vector W_Z, can be presented in the form of two groups of components. The first group forms a vector of characteristics of SISC availability SISC W_G and the second group–a vector of characteristics of systems stability W_S.

In view of restrictions, which are imposed on separate groups of vector components W, which are irrelevant and independent, the area of admissible values $\{W_D\}$ – vector can be presented in the following form:

$$\{W_D\} = \{W_{DC}\} * \{W_{DG}\} * \{W_{DH}\},$$

where $\{W_{DC}\}$ – range of admissible value of target use indexes SISC;

$\{W_{DG}\}$ – range of admissible values of characteristics of system availability;

$\{W_{DH}\}$ – range of admissible values of operational and technical characteristics of system reliability;

$*$ – sign of direct product ensemble

In this case criterion of operation efficiency (1) that estimates quality, will take a form:

$$W \in \{W_D\} = W_C \in \{W_{DC}\} \cap W_G \in \{W_{DG}\} \cap$$

$$\cap W_S \in \{W_{DS}\} = W_C \in \{W_{DC}\} \cap W_Z \in \{W_{DZ}\},$$

where $W_Z = W_G \cup W_S$ – vector of the providing characteristics of SIS complex and target process of functioning;

$\{W_{DZ}\} = \{W_{DG}\} * \{W_{DS}\}$ – range of accepted values of vector W_Z.

Efficiency index of target use of SISC which is set by probability of target achievement, will be defined by equality:

$$P_{DM} = p(W \in \{W_D\} = p(W_C \in \{W_{DC}\} * p(W_G \in$$

$$\in \{W_{DG}\} ** p(W_S \in \{W_{DS}\} = P_C P_G P_S = P_C P_D, \quad (2)$$

where $P_G = p(W_G \in \{W_{DG}\}$ – probability that at the moment of target-seeking process use of SISC, the system is ready to functionate;

$P_S = p(W_S \in \{W_{DS}\}$ – conditional probability that during target use of SISC its technical characteristics will be in the limits providing execution of target task;

$P_C = p(W_C \in \{W_{DC}\}$ – conditional probability that the objectives of the executed operation will be achieved (under condition $B \cap C$);

$P_D = P_G P_S$ – probability that during target use of SISC will be in a condition of functional availability, that is probability of high-quality operational and technical ensuring of SISC target use.

The term "capacity" is generalized concept for complex and big systems [10, 11].

To explore the goal-seeking process of SIS target use in dynamics, means the sequence realization of its phases (stages), we will enter the following designations:

probability P_S denote as P_B – index of reliability SISC,

probability P_C denote as P_Z – conditional probability of execution of the SISC target task.

Then expression (2) will take a form:

$$P_{DC} = P_Z P_G P_B.$$

At the same time for co-factors of new expression it is advisable to enter the following notions:

probability P_Z – index of functional availability of SISC;

product $P_G P_B$ – index of operational and technical characteristics of SISC availability.

So long as

$$W_C \in \{W_{DC}\} \in W_G \in \{W_{DG}\} \cap W_H \in \{W_{DH}\}$$

probability P_{DC} є unconditional probability of a stochastic event $W_C \in \{W_{DC}\}$, thus, characterizes operation achievement of the target exhaustive.

In view of the foregoing analysis, we assert that the most informative and complex efficiency index of target use of SISC is the probability P_{DC} of achievement the operation target (probability of target problem execution of SISC at the set resource restrictions) under conditions of dynamic information confrontation [12].

For an example, we illustrate the application of the selected complex indicator in a mathematical model [13].

Consider the function of dynamic vulnerability $f(x, y)$, which determines the probability of a successful attack on the software information protection. In this case, the P_{DC} – probabilistic indicator of the achievement of the SIS's target (i.e., successful counteraction to the attack) can be calculated by $P_{DC} = 1 - f(x, y)$. According to the above, Fig. 1 represents the values of the indicator for different types of SIS (SIS 1 - SIS 6) and for different range of activated resources.

Obviously, the more resources activated – P_{DC} rate increases, but its maximum value depends on the specific SIS and conditions of information confrontation.

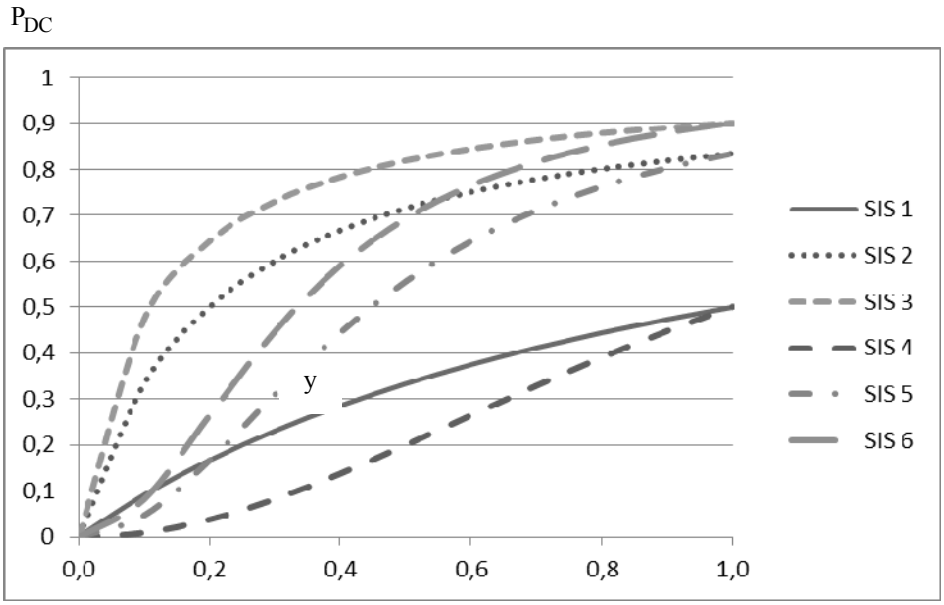

Fig. 1. Values of P_{DC} for different SIS

Conclusion

As a result of the analysis conducted in this article, additional requirements were created for the selection of indicators of the efficiency of the targeted use of these systems.

For a comprehensive research of efficiency of functioning of such a complex system the result index of quality should include three groups of the components, that are characterized by:

1) possible target effects (effectiveness of operation);

2) expenses of operational resources (resource intensity of operation);

3) time expenses (efficiency of operation).

This allowed to obtain an adequate integral indicator for assessing the efficiency of functioning of the software information security complex in the conditions of dynamic information confrontation.

Further researches should be directed to realization of automated resource management systems and dynamic change of configurations of software information security systems.

References

1. Hayden, L. (2010), "*IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*", McGraw Hill Professional, 396 p.

2. Maxwell, D. (2007), "*A Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System. Technical Memorandum*", Defence R&D Canada? Ottawa, 52 p.

3. Carin, L., Cybenko, G. and Hughes, J. (2008), "Cybersecurity Strategies: The QuERIES Methodology", IEEE Computer, Vol. 41, No. 8, pp. 20-26

4. Markoff, J. (2008), "*Leaks in Patch for Web Security Hole*", The New York Times, http://www.nytimes.com/2008/08/09/technology/09flaw.html (accessed 25 February 2018).

5. Barabanov, R. (2011), "I*nformation Security Metrics State of the Art*", DSV Report series, 56 p.

6. Rabchun, D.I. (2016), "Lohiko-dynamichna model protsesu upravlinnia resursamy zakhystu v umovakh informatsiinoho protystoiannia" [Logical-dynamic model of the process of protection resources management in the conditions of information confrontation], *Modern information security*, No. 3, pp. 62-67.

7. Rathbun, D. (2009), "*Gathering Security Metrics and Reaping the Rewards*", SANS Institute, 21 p.

8. Shevchenko, V.L. (2011), "*Optymizacijne modeljuvannja v strategichnomu planuvanni*" [*Optimizing modeling in strategy planning*], CVSD NUOU, Kiev, 283 p.

9. Reijo, M. (2013), "Quality of security metrics and measurements", *Computers & Security,* Vol. 37, pp. 78-90.

10. Platzer, A. (2010), "*Logical Analysis of Hybrid Dynamical Systems: Proving Theorems for Complex Dynamics*", Springer, 426 p., https://doi.org/10.1109/MMET.2012.6331269.10.1007/978-3-642-14509-4.

11. Moore, T., Pym, D. and Ioannidis, C. (2010), "*Economics of Information Security and Privacy*", Springer, US, 320 p., https://doi.org/10.1109/MMET.2012.6331269.10.1007/978-1-4419-6967-5.

12. Savola R. (2009), "A security metrics taxonomization model for software-intensive systems," *Journal of Information Processing Systems*, Vol. 5, No. 4, 10 p.

13. Rabchun, D.I. (2015), "Otsinka efektyvnosti informatsiinoi bezpeky z urakhuvanniam ekonomichnykh pokaznykiv" [Evaluating the efficiency of information security on the basis of economic indicators], *Modern information security*, No. 4, pp. 91-96.

Надійшла до редколегії 14.02.2018
Схвалена до друку 20.03.2018

Відомості про авторів:

Шевченко Віктор Леонідович
доктор технічних наук професор
професор Київського національного університету
імені Тараса Шевченка,
Київ, Україна
https://orcid.org/0000-0002-9457-7454
e-mail: gii2014@ukr.net

Рабчун Дмитро Ігорович
аспірант Державного університету
телекомунікацій,
Київ, Україна
https://orcid.org/0000-0002-5555-0910
e-mail: rabchundima92@gmail.com

Information about authors:

Viktor Shevchenko
Doctor of Technical Sciences Professor
Professor of Taras Shevchenko
National University of Kyiv,
Kyiv, Ukraine,
https://orcid.org/0000-0002-9457-7454
e-mail: gii2014@ukr.net

Dmytro Rabchun
Postgraduate Student
of State University
of Telecommunications, Kyiv, Ukraine
https://orcid.org/0000-0002-5555-0910
e-mail: rabchundima92@gmail.com

ВИБІР І ОБҐРУНТУВАННЯ ІНТЕГРАЛЬНОГО ПОКАЗНИКА І КРИТЕРІЇВ ЕФЕКТИВНОСТІ ЦІЛЬОВОГО ЗАСТОСУВАННЯ КОМПЛЕКСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

В.Л. Шевченко, Д.І. Рабчун

Метрики інформаційної безпеки розглядаються як важливий чинник прийняття обґрунтованих рішень щодо різних аспектів безпеки, починаючи від розробки архітектури безпеки та контролів, закінчуючи ефективністю процесів захисту інформації. Для оцінювання якості функціонування складних технічних систем, таких як комплекси програмних засобів захисту інформації, в різних умовах протистояння і впливу зовнішнього середовища, і порівняння їх між собою, використовують показники і критерії якості та ефективності.

Рівень захисту може бути забезпечений різними способами, нерівномірними між собою з точки зору їх ефективності, вартості і часових витрат на їх реалізацію. Виникає завдання вибору раціональних способів з ряду можливих на основі певних показників успішності – показників ефективності захисту. Дані показники повинні служити мірою прояву якості захисту, кількісно виражати можливість нормального функціонування системи в умовах впливу загроз різного характеру. У роботі проведений аналіз показників та критеріїв для оцінки результатів функціонування реальних комплексів програмних засобів захисту інформації. В ході цільового застосування таких складних технічних систем для досягнення мети витрачається час і залучаються ресурси. Тому якість цільового застосування не може бути повно охарактеризовано жодною з його операційних властивостей окремо. Для представлення багатовимірного вектора, котрий враховує різні операційні властивості системи, у вигляді багатокомпонентного одновимірного вектора застосовано різні види згорток. Відповідно до сформованих вимог, запропоновано інтегральний показник для оцінки ефективності цільового застосування комплексів програмних засобів захисту інформації в умовах динамічного інформаційного протистояння, що дозволяє використовувати динамічний підхід до управління ресурсами захисту інформаційних систем.

Ключові слова: *оцінка безпеки, інтегральний показник безпеки, програмні засоби захисту інформації, показники безпеки*

ВЫБОР И ОБОСНОВАНИЕ ИНТЕГРАЛЬНОГО ПОКАЗАТЕЛЯ И КРИТЕРИЕВ ЭФФЕКТИВНОСТИ ЦЕЛЕВОГО ПРИМЕНЕНИЯ КОМПЛЕКСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В.Л. Шевченко, Д.И. Рабчун

Метрики информационной безопасности рассматриваются как важный фактор принятия обоснованных решений по различным аспектам безопасности, начиная от разработки архитектуры безопасности и контролей, и заканчивая эффективностью процессов защиты информации. В работе проанализированы показатели и критерии для оценки эффективности комплексов программных средств защиты информации. Согласно сформированных требований, предложен интегральный показатель для оценки эффективности целевого применения комплексов программных средств защиты информации в условиях динамического информационного противостояния, что позволяет использовать динамический подход к управлению ресурсами защиты информационных систем.

Ключевые слова: *оценка безопасности, интегральный показатель безопасности, программные средства защиты информации, показатели безопасности.*