Asesorías y Tutorías para la Investigación Científica en la Educación Puig-Salabarría S.C.
José María Pino Suárez 400-2 esq a Lerdo de Tejada. Toluca, Estado de México. 7223898475
RFC: ATI120618V12

Revista Dilemas Contemporáneos: Educación, Política y Valores.
http://www.dilemascontemporaneoseducacionpoliticayvalores.com/
Año: VI Número: Edición Especial. Artículo no.:110 Período: Junio, 2019.

TÍTULO: Selección de sistemas de seguridad de la información para asegurar la seguridad económica.

AUTORES:

1. Ph.D. E.A. Voronin.

2. Ph.D. I.V. Yushin.

RESUMEN. El documento presenta métodos matemáticos para la selección de sistemas de seguridad de la información y algoritmos para evaluar y difundir la información y la seguridad económica, teniendo en cuenta su combinación bien equilibrada. Garantizar la seguridad de la información es el área más importante para aumentar la seguridad económica y uno de los principales problemas de la economía digital. Esta tarea es interdisciplinaria y multifacética, ya que incluye temas de integración efectiva de la seguridad económica y de la información.

PALABRAS CLAVES: Economía digital, seguridad de la información, seguridad económica, blockchain.

TITLE: Selection of information security systems to ensure economic security.

AUTHORS:

1. Ph.D. E.A. Voronin.

2. Ph.D. I.V. Yushin.

ABSTRACT: The paper presents mathematical methods for selection of information security systems and algorithms for evaluating and fore-casting information and economic security, taking into account their well-balanced combination. Ensuring information security is the most important area of increasing economic security and one of the main problems of the digital economy. This task is interdisciplinary and multifaceted since it includes issues of effective integration of economic and information security.

KEY WORDS: Digital economy, information security, economic security, blockchain.

INTRODUCTION.

Currently, cybersecurity is one of the key problems of ensuring national security. In the conditions of information and cyber wars, the assessment and selection of effective protection measures are not inferior in importance and cost to conventional and nuclear means of national defense [Schwab, 2016; Dobkina, 2018; Machado et al, 2019; Mendes & Silva, 2018].

Extensive research and development are conducted in this direction, especially on the use of artificial intelligence technologies [Biryukov, 2017; Skabcov, 2018; Abdul Rahman et al, 2018; Zare, 2015]. However, there is no established methodology for substantiation and choosing the technologies and means of ensuring economic security in the digital information space. This was due to the fact that there were not even recognized, normalized criteria for information security (cybersecurity) [Beyer, et al. 2016; Kurmanali et al, 2018; Bakhshandeh et al, 2015; Vojtik and Prozherin, 2012].

In [Voronin, et al. 2018], we proposed such a criterion and methods for its calculation. Using this criterion, one can assess the level of information security, compare the effectiveness of various security systems, but the question of choosing a cost-effective security system remains open. The solution to this problem is proposed in the present work.

DEVELOPMENT.

Results and discussion.

Definition of security as "a state of an object in which it is either not exposed to a negative impact, or successfully withstands such an impact, while continuing to function normally" is the most attractive and complete, because it reflects the properties of the environment and the system itself, which functions in this environment.

In the mathematical interpretation of such statement, the effect of the environment can be described by listing of cyberattacks with the corresponding probabilities, i.e. conditional probability of various types of attacks on the digital system.

$$V_s = \{v_i, p(v_i), i = 1..n\}, \qquad (1)$$

where v_i is a type i of attack, $p(v_i)$ is the probability of its observation, $\sum_i p(v_i) = 1$.

The property of the system to withstand cyberattacks can be characterized by the probability of preserving a given behavior under i external influences, i.e. to get an appropriate set for a variety of external influences

$$Q = \{q(v_i), i = 1..n\}. \qquad (2)$$

According to the definition of security for the i external influence, using the formula of the total probability, we obtain:

$$P_s(v_i) = \big(1 - p(v_i)\big) + p(v_i)q(v_i), \qquad (3)$$

where $P_s(v_i)$ is a probability of the system being in working condition with possible external influence v_i, $\big(1 - p(v_i)\big)$ is a probability of absence of external influence v_i, $p(v_i)q(v_i)$ is a probability that an external influence occurs, but it is successfully overcome by the system or by specialized means of its protection (antiviruses, firewalls, etc.).

If the system is attacked in several ways and any of them can lead to a loss of operability, then for the entire multitude of external influences, when any type of attack leads to a violation of the operability of the protected system, its full security can be calculated as:

$$P_S = \prod_i^n P_s(v_i) = \prod_i^n [(1 - p(v_i)) + p(v_i)q(v_i)]. \quad (4)$$

It is also possible that the loss of operability can be caused by a combination of external attacks, 2 or more. Consider the case of a combination of two external events.

Note that $1 - P_1(v_1)$ is a probability of a security breach by the first attack, $1 - P_2(v_2)$ is a probability of a security breach by the second attack, then $(1 - P_1(v_1)\big(1 - P_2(v_2)\big)$ is a probability of the first and the second attacks impact to the security breach. Consequently, security caused only by the impact of two types of attacks is equal to

$$P_S(v_1, v_2) = 1 - \big(1 - P_1(v_1)\big)\big(1 - P_2(v_2)\big). \quad (5)$$

After substitutions we obtain:

$$P_S(v_1, v_2) = 1 - p(v_1)p(v_2)\big(1 - q(v_1)\big)\big(1 - q(v_2)\big). \quad (6)$$

In case when the violation of system security occurs after *m* combinations of attacks, (6) can be represented as:

$$P_S(v_1 .. v_m) = 1 - \prod_{i=1}^m p(v_i). \quad (7)$$

If an information system can be exposed to *n* external attacks and a combination of *m* attacks is required to defeat the system, the formula for evaluating its security is

$$P_S(v_1 .. v_т) = (1 - \prod_{i=1}^m p(v_i)\big(1 - q(v_i)\big)(\prod_{j=n-m}^n [\,1 - p\big(v_j\big)(1 - q\big(v_j\big)] \quad (8)$$

If the protected system has *k* defense levels, i.e. when the aggressor has to overcome several protection levels, such as: external firewall of the local network, internal firewall of the operating system, anti-virus protection, etc., then its security is:

$$P_s = 1 - \prod_k (1 - P_{s,k}), \quad (9)$$

where $P_{s,k}$ is the security provided by the *k* defense level is calculated by the formula (8).

The economic efficiency of the information security system can be estimated by the formula of the total reduced costs:

$$F_p = R_s + Z_e + U_o, \quad (10)$$

where F_p are the total reduced costs, R_s is a security system cost, Z_e are security system operating costs, U_o are losses from information security breach.

Losses from information security breaches are calculated as:

$$U_o = \sum_i u_i (1 - P_i), \quad (11)$$

where u_i are losses from the *i* type of information security breach, P_i is the safety for the *i* type of information security breach.

If the security system is multi-component and each component provides protection from its *i* type attack, then R_s is:

$$R_s = \sum_i r_i \ , Z_e = \sum_i z_i \quad (12)$$

where r_i , z_i are the cost and expenses on operation of i type of the protection system components.

It is known that the effectiveness of an information security system depends on its cost, i.e. $P_i(r_i)$.

Substituting these ratios into the general formula for the total reduced costs, we obtain the expression for the accepted indicator of the economic efficiency of the information security system:

$$F_p(z_i) = \sum_i r_i + \sum_i z_i + \sum_i u_i (1 - P_i(r_i). \quad (13)$$

It is not difficult to notice that this functional has the only extremum or minimum point because the increase of the cost of the system reduces the magnitude of the expected economic losses from the security breach of a business entity.

This indicator builds an algorithm for choosing the optimal, in the economic sense, structure of the information security system, based on minimization of the total reduced costs by the cost of its components:

$$OptR_o = \{r_i, i = 1..n\} = argmin_{r_i}[\sum_i r_i + \sum_i z_i + \sum_i u_i(1 - P_i(r_i)]. \quad (14)$$

where $\{r_i, i = 1..n\}$ is a set of system components.

An analytical solution to this problem does not exist, since there are no explicit analytical dependencies $P_i(r_i)$. They can be found experimentally using simulation or probabilistic modeling [10].

This formula is valid when each type of attack of all possible attacks leads to economic losses, but when losses result from combining several *m* of *n* attacks, the losses from them will be calculated by

$$U_m = \sum_i^{n-m}(1 - P_{Si}) \cdot u_i, \quad (15)$$

where $(1 - P_{Si})$ is an *i* version of the successful combination of *m* attacks.

If the information protection is layered and consists of *k* levels, then the losses from the security breach are:

$$U_o = \prod_k(1 - P_k) \cdot u_o \ , \quad (16)$$

where $(1 - P_k)$ is the probability of overcoming *k* level of defense, u_o is an economic damage from information security breaches?

Accordingly, formulas (15) and (16) should be substituted into the formula of the indicator of economic efficiency of the information security system.

A particular problem is the calculation of economic losses from a security breach. For different entities of economic activity, it will be calculated using a method appropriate to their purpose. The simulation studies using the Monte Carlo method are widely applied in the economy.

The determination of the probabilities of harmful attacks is based on statistical analysis of malicious events and mathematical modeling in the form of Markov and Bayesian networks [Avi Pfeffer, 2016]. Refinement of these mathematical models is carried out by machine learning methods, both at the design stage and during the operation of information security systems [Flach, 2012].

CONCLUSIONS.

The following conclusions are provided:

1. The presented approach and mathematical methods make it possible to combine the problems of ensuring the economic and information security of eco-nomic entities in a single task.
2. On the basis of the developed mathematical methodology, it is possible to develop an empirical algorithm for choosing the structure and functionality of in-formation security systems.
3. A natural and logical continuation of this work is the research and development of mathematical models of Markov and Bayesian networks with appropriate machine learning algorithms.

Acknowledgements.

Work done by grant Russian Foundation for Basic Research 18-29-03056 «Evaluation of information and economic security by methods of machine learning in the information space of the digital economy».

BIBLIOGRAPHIC REFERENCES.

1. Rahman, Abdul; M., Abdul Kadir, H., & Wok, S. (2018). Evaluation on the installation of the automatic lane barriers (alb) by campus community. Humanities & Social Sciences Reviews, 6(2), 27-33. https://doi.org/10.18510/hssr.2018.624
2. Bakhshandeh, M., Sedrposhan, N., & Zarei, H. (2015). The Effectiveness of Cognitive-Behavioral Group Counseling to Reduce Anxiety, Marriage; Single People have to be Married in Esfahan City (2013-2014). UCT Journal of Social Sciences and Humanities Research, 3(1), 10-13.

3. Schwab, B. (2016). The Fourth Industrial Revolution, World Economic Forum, 2016, 172 p.
4. Pfeffer Avi (2016). Practical Probabilistic Programming, Manning, 2016, 456 p.
5. Flach, P. (2012). Machine Learning: The Art and Science of Algorithms That Make Sense of Data, Cambridge University Press, 2012, 396 p.
6. Machado, A. D. B., Souza, M. J., & Catapan, A. H. (2019). Systematic Review: Intersection between Communication and Knowledge. Journal of Information Systems Engineering & Management, 4(1).
7. L. Dobkina, D. (2018). The five largest cryptocurrency thefts [Pyat' krupnejshih krazh kriptovalyut] // IHODL. 16.01.2018 [link: https://ru.ihodl.com/analytics/2018-01-16/5-krupnejshih-krazh-kriptovalyut/]
8. Biryukov, A.A. (2017). Information security: protection and attack [Informacion-naya bezopasnost': zashchita i napadenie], 2nd Edition, Moscow, DMK Press, 2017, 434 p.
9. Beyer, C. Jones, J. Petoff, N.R. Murphy, (2016). Site Reliability Engineering. O'Reilly, 2016.
10. Skabcov, A. (2018). Information Systems Security Audit [Audit bezopasnosti in-formacionnyh system], Saint Petersburg, Piter, 2018, 271 p.
11. Kurmanali, A., Suiyerkul, B., Aitmukhametova, K., Turumbetova, Z., & Smanova, B. (2018). Analysis of the proverbs related to the lexemes" tongue/language". Opción, 34(85-2), 97-115.
12. Mendes, I. A., & Silva, C. A. F. D. (2018). Problematization and Research as a Method of Teaching Mathematics. International Electronic Journal of Mathematics Education, 13(2), 41-55.
13. Vojtik and V.G. Prozherin, (2012). Economics of information security [Ekonomika informacionnoj bezopasnosti], St.Petersburg, 2012, 120 p.

14. Voronin, D.N. Zakharov, Ngen Kuang Thyong, (2018). “Selection and justi-fication of the universal and normalized criterion of cybersecurity” [Obosnovanie i vybor universal'nogo i normiruemogo kriteriya kiberbezopasnosti], Naukoemkie tekhnologii, 19(11), 2018, pp.4-13.
15. Zare, Z. (2015). The benefits of e-business adoption: an empirical study of Iranian SMEs. UCT Journal of Management and Accounting Studies, 3(1), 6-11.

BIBLIOGRAPHY.

1. Kossiakoff, W.N. Sweet, S. Seymour, S.M. (2011). Biemer, Systems Engineering: Principles and Practice, Wiley-Interscience; 2 edition, 2011, 560 p.
2. Mel'nikov, S.A. Klejmenov, A.M. Petrakov, (2016). Information Security [Informacionnaya bezopasnost' i zashchita informacii], 3rd Edition, Moscow, 336 p.

DATA OF THE AUTHORS.

1. E.A. Voronin. Doctor in Science (Tech.). Professor, Leading Researcher, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Moscow, Russia, E-mail: e.voronin1@gmail.com

2. I.V. Yushin. Ph.D., and Assistant Professor at Russian Presidential Academy of National Economy and Public Administration (RANEPA), Moscow, Russia, E-mail: yushin-iv@ranepa.ru

RECIBIDO: 2 de mayo del 2019. **APROBADO:** 13 de mayo del 2019.