Resource-time Model to Increase the Security of Confidential Data

Minakov Vladimir Fedorovich
Doctor of Technical Sciences
St. Petersburg State University of Economics,
St. Petersburg,
m-m-m-m-m@mail.ru

Shepeleva Olga Yuryevna
Higher Assistant
St. Petersburg State University of Economics,
St. Petersburg,
shepeleva-olga@list.ru

Lobanov Oleg Sergeevich
Candidate of economic science
St. Petersburg State University of Economics,
St. Petersburg,
thelobanoff@gmail.com

Abstract. A mathematical model has been developed for the integrated assessment of the probability of ensuring a safe state of the company's information resources in the face of threats and dangers of unauthorized access to commercial confidential information. This model is distinguished by taking into account the influence of resource factors for ensuring information security, as well as the time factor. Based on the proposed mathematical model, the dependence of the probability of providing a protected state of the company's information resources in a given range of time and resource indicators is constructed. The high efficiency of the joint use of time and resource factors was established to increase the likelihood of a company breaking even by reducing the risk of damage resulting from unauthorized access to confidential commercial information. The possibility of using this model in the tasks of strategic management of the company is justified.

Keywords: threats, dangers, unauthorized access, model, efficiency.

I. INTRODUCTION

Modern digitalization processes extend not only to local technological operations of enterprises, but also to the interaction of economic entities. These are the procedures for generating proposals for goods, work and services by manufacturers, their choice by consumers and the formation of requests for their purchase. Thus, through digital resources, the flow of material and labor resources is provided [1, 2]. Payment for goods and services is also made more often by bank transfer (electronic payments). For this, banking services are used: payment systems, remote banking services in client-bank systems, using bank cards, etc., as well as services of closed payment systems Yandex-Money, Web-Money, etc. The share of non-cash payments is approximately equal to the share cash, and with cardholders this share is 90% (according to the Central Bank of Russia). It is also important that digital technology has transformed economic processes [3, 4]. Information and communication technologies (ICT) play a system-forming role. Thus, financial, transport, marketing aggregators have become a factor in rapprochement and convergence of participants in economic processes. It is the digital platforms of aggregators that ensure the coordination of interests of consumers and producers of goods and services, ensuring the adoption and execution of decisions on transactions, the launch of business processes, and the management of economic activity resources.

In such conditions, the opportunities for unauthorized access to material and financial resources, and, accordingly, the number of computer crimes in relation to the management of listed resources, are growing [8, 9, 10]. According to estimates by McAfee experts, the direct financial damage from computer crimes for 2018 alone exceeded $ 600 billion, and the damage, taking into account losses in reputation, disrupting transactions, respectively, lost - $ 3 trillion. Consequently, the relevance of ensuring information security in the economy is increasing. It is not by chance that interest in breakthrough information technologies, for example, distributed registries (blonchain) and cryptocurrencies, their issuers and payments using them, is growing. Similar processes are observed in smart contract systems.

II. DYNAMIC RESOURCE SECURITY MODEL IN THE DIGITAL ECONOMY

The reliability of the security system of the information resources of economic entities is predetermined by the operation of protective equipment in the face of threats and dangers of unauthorized access. The analysis of such tools [5, 6, 7, 8, 9, 10] allows us to establish that they are aimed at solving the problems of a) identification; b) prevention; c) neutralization; d) suppression; e) localization; f) destruction; g) reflection; h) containment of consequences. Each of the functional information systems that solves the named class of tasks requires the enterprise to spend on the acquisition, implementation and maintenance of computer security tools. Therefore, to solve each problem, investments are needed. Obviously, the class of remedies reduces the probability q of a computer crime k times:

$$q\_1 (R) = q\_0 / k (R\_1), q\_2 (R) = q\_0 / k (R\_1) / k (R\_2) \quad (1)$$

where R is the cost of security

For weighted average cost

$$R = (R\_1 + R\_2 +... + R\_n) / N, \quad (2)$$

we have the average value of k and, therefore, we obtain in a general form

q (R) = q_0 / k ^ R = q_0 · k ^ (- R), (3)

A, expressing the multiplicity through fixing the base of the natural logarithm of e

through the ratio

k ^ (- R) = e ^ (- R / R_o) (4)

where R_o is the numerical value of the costs, providing a decrease in the probability q by e times:

q (R) = q_0 〖· e〗 ^ (- R / R_o), (5)

The character of the dependence q (R) is shown in Fig. one.

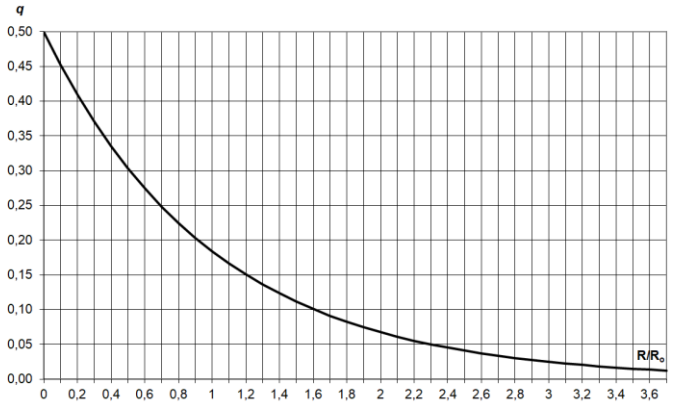

Fig. 1. The dependence of the likelihood of computer crime on the cost of information security

Figure 1 shows that information security costs asymptotically reduce the likelihood of cybercrime [9, 16]. Indeed, it is impossible to achieve absolute security with a zero value of the probability of committing malicious acts in virtual space.

Given that the sum of the probabilities of the safe operation of information resources p and the probability of the implementation of computer crimes q

q (R) + p (R) = 1, (6)

we get

p (R) = 1-q (R), (7)

Thus, the reliability indicator - the probability of failure-free operation of the protection system, is described by the dependence on the volume of resource provision with security tools: software and hardware, the development of new methods, organizational mechanisms, etc. This can be expressed by the formula:

p (R) = p_max1 · (1-e ^ (- R \ / R_o)), (8)

where: e≈2.71828,

p, p_max1 - the probabilities (current value and the maximum possible) of successfully countering the threats and dangers of committing a computer crime, and accordingly - the economic damage caused by it with the basic version of ensuring information security.

Obviously, the use of additional protective equipment in the form of innovative solutions for which no hacking tools have been created due to the unknown operation principle and characteristics of innovations increases the probability of the security state by a certain value p_max2, with p_max1 + p_max2 = p_ (max). Otherwise: p_ (max) = p_ (max) · (a_ (1) 〖+ a〗 _ (2)) In [10, p. 54, fig. 2] the "dependence of the probability of protection" is obtained in time in the form of a sigmoid. We represent the probability sigmoid as a function of the form

p (t) = p_max2 / (1 + e ^ (d-t \ / T)) (9)

where: T is the time constant of the change in the effect of protection in the conditions of use of the safety equipment;

e≈2.71828,

d is the number of time constant of the displacement of the median value of the sigmoid relative to the beginning of the reference time.

Now, taking into account the simultaneous influence of previously used protective equipment and innovative solutions, we obtain the resulting probability of protection in the form of the sum of components (as an example, we used the time constant T = 2 years as the average period between software updates in the information security system, Ro = 4, a_ (1) = 0.5; a_ (2) = 0.5):

p (t, R) = 0.5 / (1 + e ^ (4-t \ / 2)) + 0.5 · (1-e ^ (- R \ / 4)), (10)

In fig. 1, the effect of increasing the likelihood of counteracting damage from unauthorized access to commercial confidential information is visualized. As can be seen from the figure, the increase in the likelihood of protection of digital resources significantly depends on the ratio of time and resource support of information security. This allows you to lay down design decisions on the basis of solving the problem of ensuring the required level of risks, determining a ratio of resources, and, therefore, costs, and project implementation time, which is most suitable for the company's goals, project implementation capabilities in accordance with its strategy [11, 12, 13]. Moreover, the obtained dependence is a tool for constructing a scenario field for making managerial decisions to ensure a safe state of not only informational, but also financial and material resources of a company [14, 15]. Obviously, the ratio between the effects of increasing the probability of preventing unauthorized access a_ (1) and a_ (2) can be selected on the basis of the obtained model in an optimization way, when the model can be used in the integral indicators of the company's activity for a certain time.

It is important to note that the development of a resource-costing paradigm for ensuring information security by the influence of time leads to a generalized model. Indeed, substituting the only numerical value of time (for example, the current moment of time) into the proposed model leads to a particular case of solving the problem of ensuring information security, for example, during operational control. For the tasks of tactical management in the medium term, time intervals are determined by tactical objectives. To develop a strategy for the development of an enterprise security system, the model can be

used at long time intervals during which long-term goals are to be achieved.

In addition, fixing the estimated time, we obtain a model of variable solutions in terms of choosing appropriate investments in information security resources. For example, to select alternative projects offered by information security outsourcers.

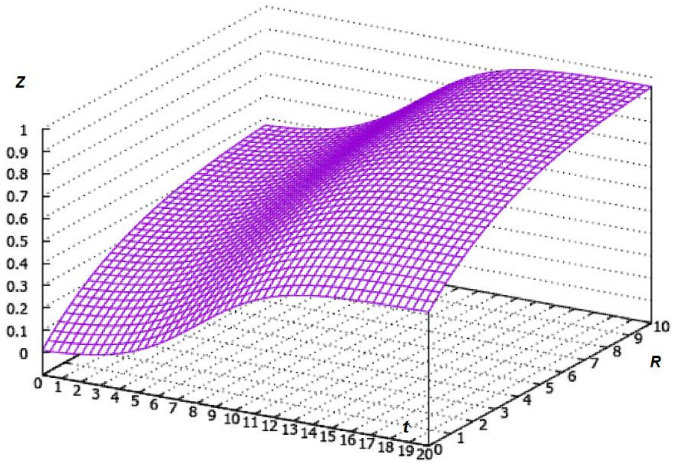

Fig. 2. The influence of resources (R) and time (t) on the probability of ensuring a safe state

The analytical type model compares favorably with the presentation of information security management processes by systems of differential equations, firstly, by the possibility of its practical use. Indeed, office applications (including cloud) allow any user to perform calculations using standard functions, for example, table processors, based on which - evaluate alternative solutions to the problem of ensuring information security. It is important that regardless of the type of protective equipment, the methods used in them, the final indicator assessed by the model is the result in the form of an assessment of the achieved probability of safe operation of the information resources of enterprises, their associations, state authorities and many other structures. The model is invariant to the types of their activities, sectors of the economy, patterns of ownership and other features.

The invariance property extends the applicability of the proposed model. It remains fair to new developments not presented on the modern market. This property is of particular value in connection with the unprecedented dynamics of the market of information and communication systems and technologies. Firstly, according to the regularity established by Gordon Moore in relation to the concentration of active keys in the microprocessor hardware and supplemented by David House with observations of the dynamics of growth in computing performance, the first and second indicators double each 18 and 24 months, respectively. Consequently, the use by attackers of more powerful computing power, even based on the simple brute force method, reduces the likelihood of maintaining a protected state of enterprise information systems. Secondly, innovative directions of digitalization of the economy based on smart technologies, processing of large volumes of data, M2M technologies, intelligent systems, cloud services, platforms and infrastructures and several others have been formed and are rapidly developing. The evolution of such information technologies makes unpredictable new places of vulnerabilities critical for economic processes. At the same time, the development of adequate methods and means of protecting information and digital business processes is being carried out taking into account new types of threats and dangers of information security in real time. The companies-developers of such tools always make offers to consumers indicating the terms of development and implementation of information protection tools, as well as the price of products. These indicators are the source data for the developed model. And its use allows, on the basis of direct calculations, to obtain quantitative estimates of the achieved result in terms of information security.

The model can also be used in addition to methods for analyzing hierarchies, decision trees, and many others in decision support systems. It is important that the development of these methods significantly develops the principles of informed management decisions taking into account the time factor. This circumstance is crucial for ensuring the sustainability of enterprises, their development.

Obviously, the time factor plays a crucial role in managing change. Its quantitative accounting allows you to change the paradigm of tactical and strategic management of the enterprise. Instead of tracking changes and following them with a lag in time, it is possible to form changes, providing the company with competitive advantages due to the primacy of the changes. It is equally important that this paradigm is in good agreement with project management methodologies. Note that the traditional project management paradigm leads, as practice shows, to low feasibility of projects. And investments in the development and implementation of projects in the economic activities of enterprises are significantly superior to investments in information security tools.

CONCLUSIONS

A model is proposed for an integrated assessment of the probability of ensuring a safe state of the company's information resources in the face of threats and dangers of unauthorized access to commercial confidential information. A distinctive feature of the model is the consideration of the time factor when using innovative solutions to ensure information security in addition to the resource factors for its increase, based on increased costs. A rather high degree of increase in the probability of breaking-even operation of the company is established, exceeding in a specific example considered the effect of the resource approach to reducing risks. The possibility of using the model in the tasks of strategic management of the company, project management of information security, as well as cost optimization. The reliability of the proposed model is confirmed by the proof of model validity by rigorous mathematical calculations.

REFERENCES

[1] Borisov, V.N., Pochukaeva, O.V. Innovative machine engineering as a factor of developing import substitution // Studies on Russian Economic Development 2015. 26(3), pp. 225-232. DOI: 10.1134/S1075700715030028

[2] Ivanter, V.V., Belkina, T.D., Belousov, D.R., (...), Yankov, K.V., Zaionchkovskaya, Z.A. Recovery of economic growth in Russia // Studies on Russian Economic Development 2016. 27(5), pp. 485-494 DOI: 10.1134/S1075700716050105

[3] Glinskiy V., Serga L., Khvan M. Assessment of environmental parameters impact on the level of sustainable development of territories // В сборнике: Procedia CIRP 13. Cep. "13th Global Conference on Sustainable Manufacturing - Decoupling Growth from Resource Use" 2016. pp. 626-631. DOI: 10.1016/j.procir.2016.01.145

[4] Glinskiy V., Serga L., Chemezova E., Zaykov K. Clusterization economy as a way to build sustainable development of the region // В сборнике: Procedia CIRP 13. Cep. "13th Global Conference on Sustainable Manufacturing - Decoupling Growth from Resource Use" 2016. pp. 324-328. DOI: 10.1016/j.procir.2016.01.050

[5] Vasil'ev, Y.S., Zegzhda, D.P., Poltavtseva, M.A. Problems of Security in Digital Production and Its Resistance to Cyber Threats (2018) Automatic Control and Computer Sciences, 52 (8), pp. 1090-1100. DOI: 10.3103/S0146411618080254

[6] Zegzhda, P.D., Poltavtseva, M.A., Pechenkin, A.I., Lavrova, D.S., Zaitseva, E.A. A Use Case Analysis of Heterogeneous Semistructured Objects in Information Security Problems (2018) Automatic Control and Computer Sciences, 52 (8), pp. 918-930. DOI: 10.3103/S0146411618080278

[7] Petrenko S.A., Makoveichuk K.A., Chetyrbok P.V., Petrenko A.S. About Readiness for Digital Economy. In Proceedings of the 2017 IEEE II International Conference on Control in Technical Systems, IEEE, CTS, 2017, pp. 96–99. DOI: 10.1109/CTSYS.2017.8109498.

[8] Olifirov, A.V., Makoveichuk, K.A., Zhytnyy, P.Y., Filimonenkova, T.N., Petrenko, S.A. Models of Processes for Governance of Enterprise IT and Personnel Training for Digital Economy. In Proceedings of 2018 17th Russian Scientific and Practical Conference on Planning and Teaching Engineering Staff for the Industrial and Economic Complex of the Region, IEEE, PTES, 2018, pp. 216 – 219. DOI: 10.1109/PTES.2018.8604166.

[9] Barabanov A.V., Markov A.S., Tsirlov V.L. Statistics of Software Vulnerability Detection in Certification Testing // Journal of Physics: Conference Series. 2018. V. 1015. P. 042033. DOI: 10.1088 / 1742-6596 / 1015/4/042033.

[10] Mal'cev G.N., Pankratov A.V., Lesnyak D.A. Issledovanie veroyatnostnyh harakteristik izmeneniya zashchishchennosti informacionnoj sistemy ot nesankcionirovannogo dostupa narushitelej. Informacionno-upravlyayushchie sistemy. 2015. No 1 (74). P. 50-58. DOI: 10.15217/issn1684-8853.2015.1.50

[11] Borisov, V.N., Kuvalin, D.B., Pochukaeva, O.V. Improving the Factor Efficiency of Machinery in the Regions of the Russian Federation // Studies on Russian Economic Development 2018. 29(4), pp. 377-386 DOI: 10.1134/S1075700718040044

[12] Litvintseva G.P., Glinskiy V.V., Stukalenko E.A. Interregional differentiation of population incomes in russian federation in the post-crisis period // Academy of Strategic Management Journal. 2017. T. 16. № 4.

[13] Glinskiy V., Serga L., Novikov A., Bulkina A., Litvintseva G. Investigation of correlation between the regions sustainability and territorial differentiation // Procedia Manufacturing. 2017. T. 8. C. 323-329. DOI: 10.1016/j.promfg.2017.02.041

[14] Borisov V.N., Pochukaeva O.V. Investment and innovative technological efficiency: case study of the arctic project // Studies on Russian Economic Development. 2017. T. 28. № 2. C. 169-179. DOI: 10.1134/S1075700717020022

[15] Ivanter V.V., Belkina T.D., Belousov D.R., Blokhin A.A., Borisov V.N. et al. Recovery of economic growth in Russia // Studies on Russian Economic Development. 2016. T. 27. № 5. C. 485-494. DOI: 10.1134/S1075700716050105

[16] Dorofeev A.V., Markov A.S., Tsirlov V.L. Social Media in Identifying Threats to Ensure Safe Life in a Modern City, *Communications in Computer and Information Science*, 2016, vol. 674, pp. 441-449. DOI: 10.1007/978-3-319-49700-6_44.