Matrix approach to risk management in the national security system, highlighting the criteria for choosing the optimal strategy for decision making

Olha Salnikova, Larisa Rodchenko, Taliat Bielialov, Margarita Skrypnyk, Larysa Ivanchenkova, Olha Slobodianiuk

Abstract*: *The emergence of new information technologies always brings not only new opportunities for optimizing interaction processes but is also accompanied by the emergence of new threats to national security, which, if ignored, can negate the potential benefits of introducing these technologies. Timely assessment of such risks and the development of adequate countermeasures are the cornerstone of progress. The introduction of artificial intelligence technology is considered as one of the incentives for the development of business and the economy as a whole. However, the use of self-learning neural networks as the primary way of implementing this technology generates completely new, not previously considered types of threats.

Index Terms*: *national security system, risk, uncertainty, matrix approach, optimal strategy, decision making.

I. INTRODUCTION

With the development of Internet technologies and e-commerce, more and more threats to national security are emerging every day. Today, organizations are increasingly using information in business processes to facilitate management decisions and business. Dependence on the information in the business environment is substantial, since a lot of trading operations are carried out electronically through the Intranet. Such information dependence has led to a significant increase in the impact of the security of information systems on success, and sometimes just the possibility of doing business. Therefore, the security of information systems is one of the most important issues [1], which attracts much attention from analysts, engineers and other professionals in the field of information security. Thus, on the one hand, risk assessment plays a vital role in the stable functioning of national security, but, on the other hand, most methods and models of such an assessment have shortcomings. Some of them are only qualitative methods of analysis, some – merely quantitative, cumbersome for implementation. These traditional methods of evaluation have a lot of personal problems and inaccuracies, so they are quite complicated in application.

II. FORMULATION OF THE PROBLEM: RISKS AND THREATS TO NATIONAL SECURITY DUE TO THE DEVELOPMENT OF THE DIGITAL ECONOMY

Unbalance, uncertainty, multicriteria are typical signs of a market economy that is always accompanied by risks. Entrepreneurship and risk are organically interconnected phenomena in a market economy [2].

In general, the scientific achievements of scientists on risk issues are significant. The use of quantitative and qualitative methods for assessing the risks of business activity has its advantages and disadvantages and is limited to the experience.

New technologies involve the use of specific equipment and software. If the development of such end-to-end technologies will not be accompanied by the creation of a corresponding domestic production base that would ensure their implementation, a sharp increase in import dependence is possible due to the need to import foreign components and devices.

The digital economy is currently associated primarily with the development of many end-to-end technologies, such as big data, neurotechnology, artificial intelligence, a distributed registry system (blockchain), the industrial Internet, and sensory.

A. Personal data and broad user data

The digitization of any activity is accompanied by an increase in the amount of information stored, transmitted and processed, which poses a threat to the protection of confidential data, in particular, personal data of users [3]. Currently, there is a problem of protecting extensive user data, that is, heterogeneous information about user behaviour (so-called profiles) collected by devices and services in the network for a long time. Such data, although initially not personal, in the aggregate and with additional processing, allow you to recover personal data of users. The

Revised Manuscript Received on June 14, 2019.

Olha Salnikova, Educational and Research Center of Strategic Communications in the sphere of National Security and Defense, National Defense University of Ukraine named after Ivan Cherniakhovskyi, Kyiv, Ukraine

Larisa Rodchenko, Eastern European Slavic University, Uzhgorod, Ukraine

Taliat Bielialov, the Finance and Financial and Economic Security Department, Kyiv National University of Technologies and Design, Kyiv, Ukraine

Margarita Skrypnyk, Department of Accounting and Auditing,Kyiv National University of Technology and Design, Kyiv, Ukraine

Larysa Ivanchenkova, Department of Accounting and Audit, Odessa National Academy of Food Technologies, Odessa, Ukraine

Olha Slobodianiuk, Department of Finance, Banking and Insurance, Odesa Institute of Trade and Economics of Kyiv National University of Trade and Economics, Odessa, Ukraine

development of technologies makes it possible to collect such information not only for special services but also for commercial organizations, the latter actively selling it.

B. Artificial Intelligence

The introduction of artificial intelligence technology is considered as one of the incentives for the development of business and the economy as a whole. However, the use of self-learning neural networks as the primary way of implementing this technology generates completely new, not previously considered types of threats [4]. Currently, a field of research is emerging that is related to ensuring the safety of learning processes and the functioning of self-learning neural networks. Since the neural network is determined by both the source code and the data entered into it in the learning process, situations are possible when the intruder influences the learning process, trying to generate input data that will be classified incorrectly, or in the learning process provides specially formed data leading to improper network training (data poisoning). There are no effective methods to counter such attacks.

C. Blockchain

The blockchain technology, widely discussed today, is a prime example of an attempt to find new interaction paradigms in the digital world [5].

The greatest vulnerability of the blockchain is the very question of how to implement the blockchain. For most modern variants of its application, the answer to the question of whether it is possible to achieve a similar system without a blockchain will be definite. Moreover, as the analysis shows, the decentralized blockchain in its current form is not suitable for use in large-scale high-loaded systems due to natural limitations on performance (difficulty of reaching consensus and the need to store large amounts of data).

In the case of using its (partially) centralized options, information systems are close in their functional characteristics to those currently used.

From the point of view of information security issues, two aspects need to be considered - theoretical and practical.

Security Consensus Protocols.

The theoretical one is primarily associated with the general scientific lack of substantiation of the security of consensus protocols. For the oldest bitcoin protocol used in cryptocurrency, the Proof-of-Work protocol currently offers a large number of different attacks, some of which can be implemented quite simply. Most of them are related to the absence of a control centre and are based on the impact on network protocols and changes in the internal network traffic parameters: Punitive and Feather Forking, Transaction Malleability, Sybil, DDoS, Eclipse, Tampering. Transaction confirmation nodes (miners) can also act contrary to the rules of the system: attack 51%, buying a miner, changing the system time of a miner, Selfish Mining, Finney Attack.

Other options for achieving consensus, such as Proof-Of-Stake, Delegated Proof-Of-Stake, Proof-Of-Space, which are under active consideration, have an even more significant number of vulnerabilities or are poorly understood.

In general, it is not yet fully understood what a secure consensus protocol should be to ensure stable operation of the blockchain system for a long time, taking into account the possible impact of violators.

The introduction of artificial intelligence technology is considered as one of the incentives for the development of business and the economy as a whole. However, the use of self-learning neural networks as the primary way of implementing this technology generates completely new, not previously considered types of threats.

Practical safety

From a practical point of view, modern blockchain systems developed by enthusiasts often have serious vulnerabilities that allow hacker attacks to be carried out. This is more true for the field of cryptocurrency. The attacks on cryptocurrency exchanges (Mt. Gox, Bitfinex, Coincheck, etc.) and individual users, aimed primarily at stealing data from cryptocurrency wallets, are widely known.

The attempt to use the blockchain outside a closed digital environment, for example, for registering real estate objects, controlling the movement of goods, raises the question of the legal significance of registration actions. Even without considering the regulatory and organizational-technical issues of the use of electronic signatures, in this case, the critical issue is the reliability of registration in the system of events or objects occurring in the real (physical) world. This is an extremely problematic issue for existing systems, which remains in the case of blockchain technology. At the moment, there are no trusted methods of such (automatic) registration. Many researchers attribute the issue of blockchain implementation to the solution of the problem of developing such techniques.

D. Internet of Things and Sensory

The question of the trusted entry of information into the blockchain is in direct contact with the concept of the Internet of things, which has existed since 1999. Despite its long history, critical security issues in this area have not yet been resolved. Numerous examples of critical attacks on devices connected to the Internet are widely known. In particular, everyone knows the story of the Mirai botnet, which used IoT devices to organize DDoS attacks [6].

At the same time, many security principles widely used in classical cryptography do not work in the world of the Internet of things: the ability of an intruder to directly access a device makes it difficult to use secret keys, securely storing key certificates.

As a result, there are severe difficulties with the trusted identification/authentication of IoT devices, the implementation of secure update mechanisms and ensuring the reliability of obtaining information from such devices.

At the same time, the existing national standards of the Russian Federation in the field of cryptographic protection of information sufficiently meet the operational requirements imposed by the characteristics of the Internet of things devices. The encryption algorithm "Magma" is one of the world leaders among low-resource algorithms in terms of efficiency of implementation and the provided durability margin.

The most challenging issue for the Internet of Things is the widely used cryptographic protocols that require the transfer of significant amounts of service fields, which is often highly undesirable for devices with limited resources.

The digital economy is currently associated primarily with the development of many end-to-end technologies, such as big data, neurotechnology, artificial intelligence, distributed registry systems (blockchain), the industrial Internet, and sensor technology.

E. Biometric identification / authentication

Biometric identification and authentication are currently another of the actions discussed technologies. However, the biometric identification/authentication system, consisting of the biometric image reading subsystems, biometric image processing, biometric data storage, comparison and decision making, due to its complexity and heterogeneity of the mechanisms used, allows offenders to implement new attack vectors.

The following problem points can be distinguished(will be used in the example):

1) dependence of recognition accuracy on the resources involved and the characteristics of the equipment;

2) the possibility of creating artificial biometric images;

3) possibility of synthesis of biometric parameters (for example, with remote biometric identification);

4) intentional modification of biometric characteristics;

5) the difficulty of preserving the biometric characteristics in secret and their inalienability in the event of a compromise;

6) the impact of actual operating conditions on the quality of recognition;

7) the possibility of leakage or change of stored biometric parameters.

It is essential that for biometrics, like no other technology, the development of recognition methods (synthesis of biometric systems) entails the corresponding development of threats.

In this regard, to consider biometrics solely as the only alternative to existing methods of identification/authentication is impractical.

The issue of inalienability of biometric data requires the development of stringent measures to ensure the safety of their processing and storage by operators, especially when implementing the national biometric platform currently being developed.

III. Review of Existing Approaches to Risk Assessment Modelling

There is no rigorous classification for risk analysis methods, but there are differences in approaches to risk analysis, ways of presenting risk elements, functionality, etc. Based on these differences, you can distinguish three main groups - graphic, mathematical and linguistic methods.

Graphic methods - methods that provide visualization of objects of analysis and processes of interaction between them. In this case, graphs, trees or diagrams are constructed that allow different way to display information about the objects being studied. In most cases, these methods only allow identification of risk elements and how to interact with them.

Mathematical methods are methods that provide the definition of properties of objects and their interaction with the help of some formal languages of description, defining the laws of functioning, change of properties, etc. These methods allow not only to identify the elements but also to analyze their behaviour, change their properties and influence on other factors. Linguistic methods are the most popular and easy to use, but not always able to lead to an adequate assessment of the situation. These methods do not provide any tools and programs and require only the presence of a team of persons responsible for risk analysis. At the same time, all stages of risk assessment, to the extent possible, involve only oral communication between a group of individuals, during which elements of risk are identified, assumptions about their behaviour are being built and an approximate assessment of opportunities and losses is made.One of the first interpretations of the approach to risk measurement was suggested by Milton Friedman [7]. He considered the problem of calculating (estimating) the level of risk through the prism of the theory of utility. Friedman noted that in the context of declining efficiency and danger, the usual maximization principles could not be used since a specific tax is required in the form of compensation for the risk factor. Friedman classified the risk-related decisions as follows: a small risk associated with a previously known outcome; moderate risk without high income and expenses; the high risk associated with high profits or losses. Friedman proceeded from the assumption that the economic unit has a specific system of advantages, which can be described by a function that gives a numerical value to various alternatives. Unfortunately, the very essence of the risk methodology poses some difficulties in its practical application, because it requires the calculation of high-precision estimates of information risks, operation with them and requires the need for a particular individualization, the exclusivity of the solutions obtained in this approach.

IV. Methodology: Application of the Matrix Method in Practice

A. Algorithm

The risk management matrix includes for the category and suggests that for each risk, the type of damage is determined and the probability of such damage occurring [8] (Table 1).

Table 1. Verbal and Numeric Risk Scales

Severity		
Verbal	Numeric	Description
Catastrophic	5	Likely to result in death
Critical	4	Potential for severe injury
Moderate	3	Potential for moderate injury
Minor	2	Potential for a minor injury
Negligible	1	No significant risk of injury
Frequency		
Verbal	Numeric	Description
Frequent	5	Hazard likelyto occur
Probable	4	Hazard will be experienced
Occasional	3	Some manifestations of the hazard are likely to occur

Remote	2	Manifestations of the hazard are possible but unlikely
Improbable	1	Manifestations of the hazard are very unlikely

You then plot the numbers on a matrix or chart, with each square calculated as the product of the corresponding frequency and severity level (Fig. 1) [9].

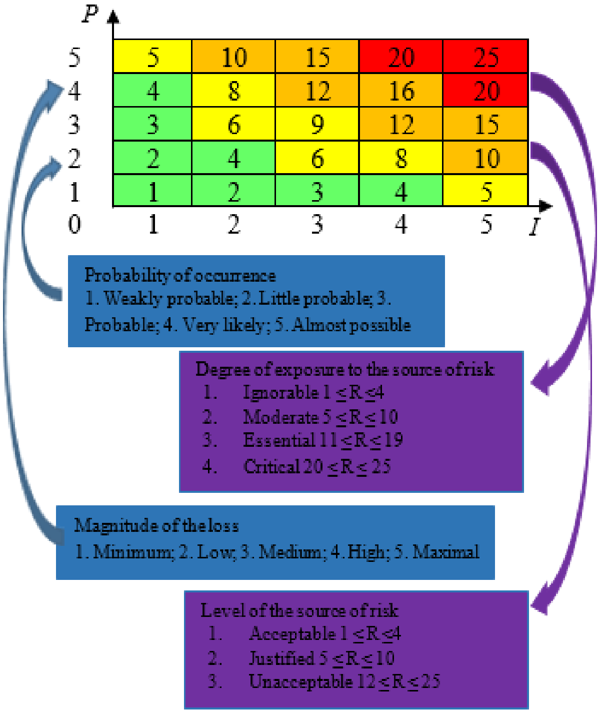
P
I
0
1
2
3
4
5
5 10 15 20 25
4 8 12 16 20
3 6 9 12 15
2 4 6 8 10
1 2 3 4 5
Probability of occurrence
1. Weakly probable; 2. Little probable; 3. Probable; 4. Very likely; 5. Almost possible
Degree of exposure to the source of risk
1. Ignorable 1 ≤R≤4
2. Moderate 5 ≤R≤10
3. Essential 11≤R≤19
4. Critical 20 ≤R≤ 25
Magnitude of the loss
1. Minimum; 2. Low; 3. Medium; 4. High; 5. Maximal
Level of the source of risk
1. Acceptable 1 ≤R≤4
2. Justified 5 ≤R≤10
3. Unacceptable 12≤R≤25

Fig 1. Risk assessment matrix

The final step is to prepare a risk report, which should include risk management measures to make informed management decisions.

B. Practical use

The construction of the matrix will show on the example of biometric identification/authentication (Fig. 2, Table 2).

🟨	🟧	🟧 3	🟥 7	🟥
🟩	🟨 1	🟧	🟧 6	🟥 5
🟩	🟨	🟨 4	🟧	🟧
🟩	🟩	🟨	🟨 2	🟧
🟩	🟩	🟩	🟩	🟨

Fig 2. Sample Risk Report

Table 2. Sample risk reduction measures

Event	Damage	Probability	Risk	Manageability	Measures
7. the possibility of leakage or change of stored biometric parameters	High	High	🟥 High	Average	Enhance physical security measures. Additional data coding. Internet access restriction
4. Intentional modification of biometric characteristics	Average	Average	🟨 Average	Average	Add parameter for the user, which is part of him
…	…	…	…	…	…
…	…	…	…	…	…

C. Analysis of the results

The risk map allows to:

Provide an overall picture of the leadership.

Properly prioritize the allocation of resources for risk management.

Disclose information about risks external to interested parties.

Distribute responsibility for risks among managers.

V. CONCLUSION

This article presents a convenient methodology for managing national security risks that organizations can easily use. The methodology provides suitable templates that can gradually improve with the amount of available information. The methodology ensures transparency, of the analysis process. Using the matrix method allows you to adapt to ever-changing threats, vulnerabilities and assets.

REFERENCES

1. Kenneth J. Knapp, Thomas E. Marshall, R. Kelly Rainer, Jr., and Dorsey W. Morrow. The Top Information Security Issues Facing Organizations: What Can Government Do to Help?, Information security and risk management,pp. 51-58, 2006
2. S. Sellami, T. Dkaki, N. E. Zarour, P.-J. Charrel. MidSemI: A Middleware for Semantic Integration of Business Data with Large-scale Social and Linked Data, International Journal of Information System Modeling and Design, 10(2), pp. 1-25, 2019
3. Bondarenko S., Liganenko I., Kalaman O., Niekrasova L., “Comparison of Methods For Determining The Competitiveness of Enterprises To Determine Market Strategy”, International Journal of Civil Engineering and Technology (IJCIET), 9(13), pp. 890-898, 2018

4. Jung-seop Youm. Commercialization of Artificial Intelligence and Artificial Intelligence, http://doi.org/10.22255/JKABS.85.3, 2018
5. I. Bashynska, M. Malanchuk, O.Zhuravel, K. Olinichenko, Smart Solutions: Risk Management of Crypto-Assets and Blockchain Technology, International Journal of Civil Engineering and Technology (IJCIET) 10(2), pp. 1121–1131, 2019
6. Ramirez, A.R.G., González-Carrasco, I., Jasper, G.H. et al. Computing (2017) 99: 107. https://doi.org/10.1007/s00607-016-0529-2
7. FriedmanMilton, The Use of Ranks to Avoid the Assumption of Normality Implicit in the Analysis of Variance, Journal of the American Statistical Association, 32, pp. 675-701, 1937
8. Lagodiienko V., Malanchuk M., Gayvoronska I. and Sedikov D. Selection of criteria for key performance indicators by the matrix method, International Journal of Mechanical Engineering and Technology, 10(1), pp. 1303-1311, 2019
9. Bashynska I., Filyppova S. Risk Management. Practical lessons & Case Study: textbook, Kharkiv: “Disa Plus”, 220 p., 2018