BLOCKCHAIN TECHNOLOGY BASED SYSTEM-DYNAMIC SIMULATION MODELING OF ENTERPRISE'S CYBER SECURITY SYSTEM

Mustafa Sadigov
Azerbaijan State University of Economics (UNEC)
Baku, Istiqlaliyyat str., 6, AZ1001, Azerbaijan
must.sadigli@gmail.com

Olha Kuzmenko
Sumy State University
Sumy, Rimsky-Korsakov str., 2, 40007, Ukraine
o.kuzmenko@uabs.sumdu.edu.ua

Hanna Yarovenko
Sumy State University
Sumy, Rimsky-Korsakov str., 2, 40007, Ukraine
a.yarovenko@uabs.sumdu.edu.ua

ABSTRACT

This research is devoted to solving the issue of increasing the level of cybersecurity in large companies through the introduction of modern blockchain technology. The urgency of this problem has been determined for enterprises that have faced with cases of cyber fraud, initiated not only by hackers but also by company employees. The authors have proposed a system-dynamic model of the company's cybersecurity system built using blockchain technology. The choice of this modeling tool gives an ability to create a computer model of a complex cybersecurity system for further effective design of the proposed modification. The authors have made the main emphasis on reducing the threat associated with the human factor since, according to statistics, 34% of cases are accounted for by the system vulnerability due to user activities. The researchers have developed a diagram of causal relationships, which imitates the process of personnel behavior in the environment of an enterprise automated information system, provided that a person intentionally or unintentionally carries out fraud. The model takes into account the primary condition when any transaction initiated by a person registered in the system has fixed in its blockchain. Thus it reflects the system reaction in case of illegal actions, which further creates the basis for the development of a set of preventive measures. The authors have proposed a system-dynamic diagram based on an analysis of the causal relationship diagram. The article describes the components of the model in the form of differential equations and conducted experimental modeling for various values of some parameters at the initial level of others to identify the sensitivity of the system. The results have made it possible to conclude about the increasing system response in cases of employee fraud in the environment of the company's automated information system if it bases on blockchain technology.

Keywords: *blockchain, cybersecurity, enterprise information system, fraud, system-dynamic simulation modeling*

1. INTRODUCTION

Most companies face such a problem as decreased reliability of the cyber security system, which leads to vulnerabilities in the corporate information system of enterprises and violation of the confidentiality, integrity and availability of data. In the modern world, such problems usually lead to the loss of information, and, as a result, companies lose their customers, money,

and reputation. This is due to the intervention of external cyber fraudsters who aim to steal information, including personal data of clients and banking information. Cybercrime cases are often committed by enterprise employees who have unlimited access rights, use remote access, mobile applications, and cloud technologies. Therefore, companies are interested in creating an effective cybersecurity system that would reduce the number of incidents and prevent cyber threats. The practice shows that despite the growing investment in the development of a cybersecurity system, current data protection solutions do not meet the needs of the business. This conclusion was reached by 81% of respondents surveyed by Dell Technologies. The main reason is the increase in the amount of information owned by companies. In 2019, its volume grew by almost 40% as compared to 2018 with a total cost of data loss of more than $1 billion per organization (DELLTechnologies, 2020). According to the IBM study, about 60% of initial cases of penetration in the company's information system was due to account data that were previously stolen (29% of cases that led to the loss of 8.5 billion records), or software vulnerabilities (more than 30% of cases) (IBM Security, 2020). On the other hand, 34% of cases are accounted for by the system vulnerability due to user activities (EY, 2018). The problem of improving the efficiency of the cybersecurity system of enterprises is global. The average amount of financial losses from information leaks in June 2019 for medium-sized businesses in the world amounted to about $3.92 million (Ponemon Institute, 2019). Therefore, companies are interested in attracting the latest technology to ensure the reliability and security of information. The following technologies were widely used in 2019: Cloud-native Applications (60%); Artificial Intelligence and Machine Learning (64%); Software-as-a-Service Applications (54%); 5G / Cloud Edge (infrastructure) – 67%; Containers – 48%. However, the problem exists and its consequences are not reduced. Thus, there is a need to involve other approaches. Although, according to the survey (DELLTechnologies, 2020), 71% of respondents believe that new technologies create a greater complexity of data protection, while 61% state that they pose a risk to data protection. In our opinion, companies should pay attention to blockchain technology, which has proven itself to be effective in the financial sphere. This confirms the growth of investment in developers of corporate blockchain solutions, which in 2019 reached almost $434 mln, which is by 62% higher than the investment in 2018 (Ledger Insights, 2020). The analytical platform CB Insights identified 58 industries where blockchain can be used, including cybersecurity (CBINSIGHTS, 2020). Goldman Sachs experts believe that due to the introduction of this technology, the probability of cyber hacking is reduced during data transfer because blockchain provides for open registries, advanced cryptography methods, and has powerful cyber protection as compared to traditional systems (TADVISER, 2020). Since the team of authors believes in the prospects of using blockchain technology to increase the reliability of the cyber security system of enterprises, this study used a system-dynamic modeling of a system that uses blockchain technology and a traditional information system to compare their effectiveness.

2. LITERATURE REVIEW

Analysis of data from the Scopus database showed that the publication activity on the topic of cybersecurity has increased by 17.67 times over the past ten years, which indicates a growing interest in it. This trend is observed in scientific papers on blockchain technologies, which have been actively studied since 2016. Over the past four years, the number of publications on this topic has grown by 30.93 times, due to the emerging prevalence of this technology in various fields, especially Computer Science and Engineering. The authors have formed a bibliometric map using the VOSviewer software product (VOSviewer, 2020), which made it possible to analyze scientific studies that reveal the possibilities of using blockchain technology to solve cybersecurity problems. The map was built based on publications from the Scopus database on cybersecurity and blockchain.

It reflects 6 clusters of publications according to keywords (Figure 1). Scientists who consider issues related to blockchain and cybersecurity study them in conjunction with financial markets, cryptocurrencies, the Internet of things, and electronic money. They solve the problems of malware, data protection, authentication, and peer to peer networks that arise in these areas since they require powerful methods of information protection. The second cluster combines blockchain, cryptography, electronic data interchange, smart contracts, smart grid, smart power grid, and commerce, i.e. scientists focus on the software and technical aspect of blockchain technology and its implementation in the field of commerce. When analyzing other clusters, they highlight a wide range of technologies that are associated with the possibility of using blockchains in cybersecurity systems: artificial intelligence, deep learning, intrusion detection systems, machine learning, 5G mobile communications, big data, cloud computing, edge computing, etc.

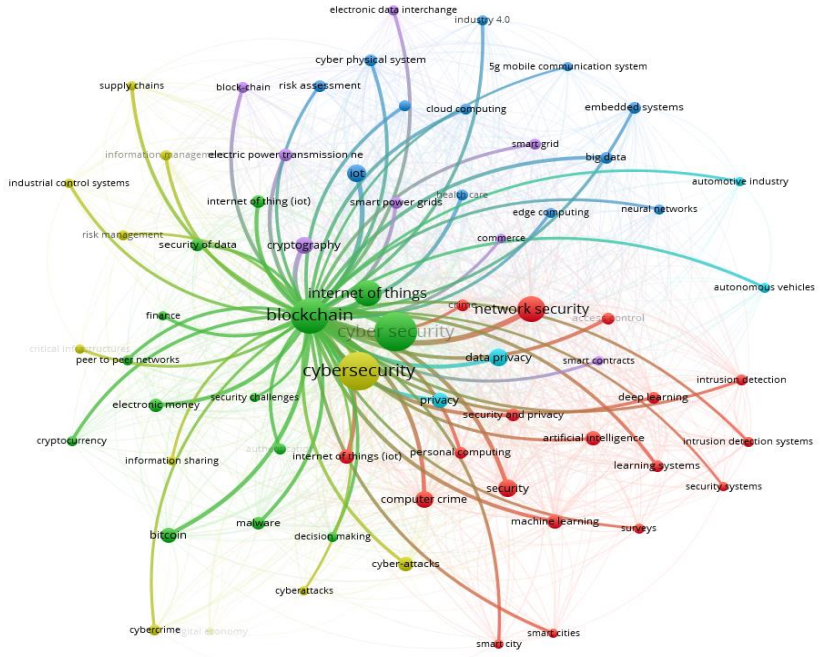

Figure 1: Bibliometric map based on keywords
(Source: original development)

Scientists study various aspects related to cybersecurity. The issue of digitalization of business processes is relevant, which contributes to increasing requirements for cybersecurity systems. This occurs under the impact of Industry 4.0 on entrepreneurship in developed and developing countries (Tapscott, Tapscott, 2016**;** Kendiukhov, Tvaronavičienė, 2017; Bilan et al., 2019b). It is also one of the main prerogatives of the state since the consequences of cybercrime affect the state's economic security system, which requires certain regulatory measures (Levchenko et al., 2019; Grenčíková et al., 2019). Some authors (Rios et al., 2018) condemn the rapid pace of digitalization and automation of companies, noting that this leads to the fact that such technologies turn into a factor that is destructive rather than integrating, and contributes to the emergence of new cyber threats for companies and states in general. Another group of authors (Bilan et al., 2019c; Grytsenko et al., 2010; Rubanov et al., 2019) highlights the relationship between the amount of funding and the level of development of information technologies. Since the need to ensure the reliability of the cybersecurity system is growing, there is a need for further improvement and development of investment mechanisms for projects such as the introduction of blockchain technology in the activities of companies (Levchenko et al., 2018; Sotnyk et al., 2020; Choo, et al., 2020).

One of the problematic aspects related to cybersecurity is the human factor, i.e. the participation of a person in the commission of a crime aimed at embezzlement, destruction or distortion of information. Researchers (Korablinova, 2017; Grytsenko, Vysochina, 2012; Berzin et al., 2018) note that today a human has become a part of a complex information system, which increases its intellectual capabilities towards unauthorized interference in the system. This idea is also supported by scientists (Bilan et al., 2019a; Pakhnenko et al., 2018). As indicated in the paper (Cosmulese et al., 2019), the digital revolution affects various aspects of life, including the level of people's awareness of cybersecurity issues. This impact, on the one side, is an incentive for the development of IT literacy, according to scientists (Vasylieva et al., 2017b), and on the other side, this will contribute to the emergence of new forms of cyber fraud, which is one of the threats. In the paper (Leonov et al., 2017), it is argued that the level of organization of information systems affects the level of development of the company. This leads to the fact that ERP-class systems in combination with artificial intelligence systems, Internet of things systems, cloud technologies, which corresponds to the level of a leading company, contribute to increasing the reliability of their cybersecurity system. This is also relevant for banking institutions that are faced with massive cyberattacks, social engineering; therefore, they are interested in developing modern anti-fraud means (Boiarko, Samusevych, 2011; Druhov et al., 2019; Vasylieva et al.). Thus , the use of modern mathematical methods (Lyeonov et al., 2019), new approaches to the development of modern engineering knowledge, creation and construction of databases and knowledge bases (Melnyk, 2017; Drescher, 2017), and methods for identifying IT risks (Semenova, Tarasova, 2017) are promising areas for solving this issue. This study, taking into account the experience of other authors, will consider the prospect of using blockchain technology to reduce the vulnerability of the company's information system and increase the reliability of the cyber security system.

3. RESEARCH METHODOLOGY

The method of system-dynamic modeling was chosen for the research. Its main advantage is the ability to model the behavior of systems at a high level, based on their information and logical structure and based on a data-flow approach. The research methodology includes the following stages:

- Stage 1 – development of a cause and effect diagram. For this purpose, the main elements of the system were identified: the intention of a person to commit cybercrime; influencing factors for increasing or decreasing cybercrime; human actions for committing cybercrime (unauthorized access, copying, destruction and modification of information, user errors, intentional non-preservation of information); recording data in the blockchain and database of a traditional information system; user features, company policies, and system vulnerabilities. Cause and effect relationships were established between the main elements, which, together with certain elements, formed the parameters of the system. A cause and effect relationship is positive if an increase (decrease) in the parameter affects the increase (decrease) of the parameter that is affected, or negative when an increase (decrease) in the parameter affects the decrease (increase) of the parameter that is affected.
- Stage 2 – development of the flow chart. At this stage, levels were identified, i.e. parameters that are influenced by a larger number of other parameters, taking into account the positive and negative effects. Special parameters were taken into account, i.e. those that cause the corresponding level to increase or decrease. Additional variables and constants were also used. For each variable was set an equation.
- Stage 3 – setting system parameters and test simulation. For this purpose, limit values are set for the initial parameters, which show the state of the system as a result of a person's intentions to commit cybercrime. The following parameters require changes: a ban on downloading information, a ban on opening and launching unknown files, a ban on the use

of external media, limited access, hardware errors, database openness, remote access. If the need arises, then the appropriate levels are debugged. Then the simulation is performed, resulting in a visualization of the system's behavior when there are potential intentions to commit cybercrime; the system's reactions are determined in the case of recording data in the blockchain and in the case of using a traditional information system. In the end, we get a result that shows the reaction of the system to its vulnerabilities in the case of using blockchain technology and a traditional information system.

4. RESULTS

System-dynamic modeling was performed in the Vensim environment, which is used for scientific purposes to implement this type of simulation (Ventana Systems, 2015). As a result, a cause and effect diagram (Figure 1) was constructed, which reflects the logic of the functioning of flows between the elements of the system.

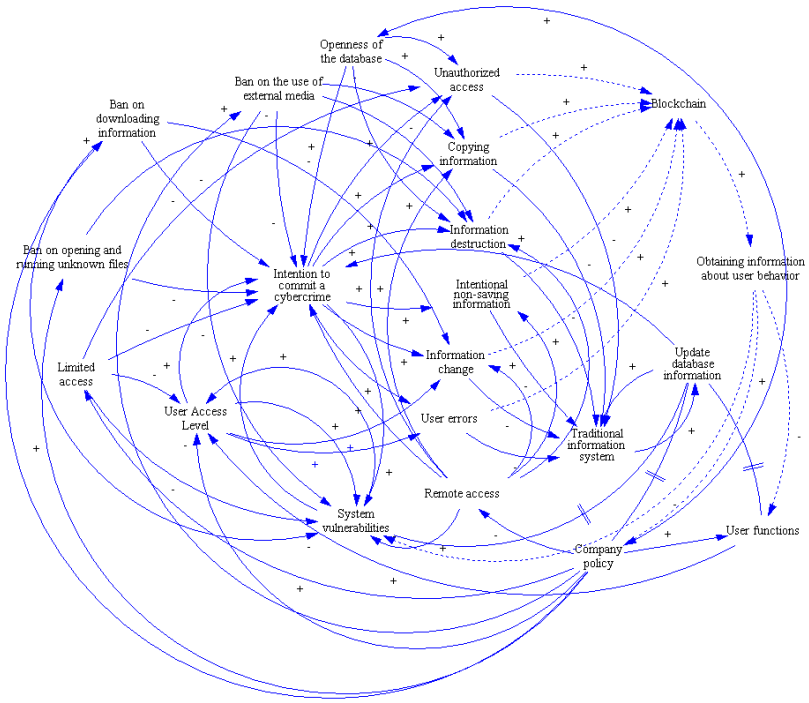

Figure 2: Cause and effect diagram
(Source: original development)

The main element is the "intention to commit cybercrime". The state of this element is affected by the following factors: a ban on downloading information, a ban on opening and running unknown files, a ban on using external media, restricted access, the level of user access, database openness, and remote access. Depending on the state of these factors, the intention may increase if the user is aware of the absence of such prohibitions, or has unlimited access rights, etc. The intention may decrease in cases where the company has a high level of protection, establishes various prohibitions, grants access rights in accordance with the functional responsibilities of the employee, etc. The model assumes that a cybercriminal intends to steal information by copying it, or destroy data or change information, or perform intentional non-saving, unauthorized access, or distort information by making errors. These activities are selected as the most popular illegal actions that contribute to the emergence of vulnerabilities of a system and reduce the level of its cybersecurity. If the blockchain technology is implemented in the company, it provides that all actions are recorded in the blockchain and are not subject to any changes.

Accordingly, using an artificial intelligence system, blockchain data can quickly provide information about user behavior and, as a result, detect violations. The model assumes that the recording occurs in a traditional information system, but if the information is updated, the recording in the system may not be saved. The cybersecurity system will need quite a long time to check activity logs to detect violations. Depending on the results, the company's policy, user functions, and the state of system vulnerabilities are changed, which affects the intention to commit cybercrime. At the second stage, a flow diagram was obtained (Figure 3), which was constructed using the mathematical apparatus represented by a system of equations (formula 1). The notation for the variables from the system of equations is signed for each element in the figure 3.

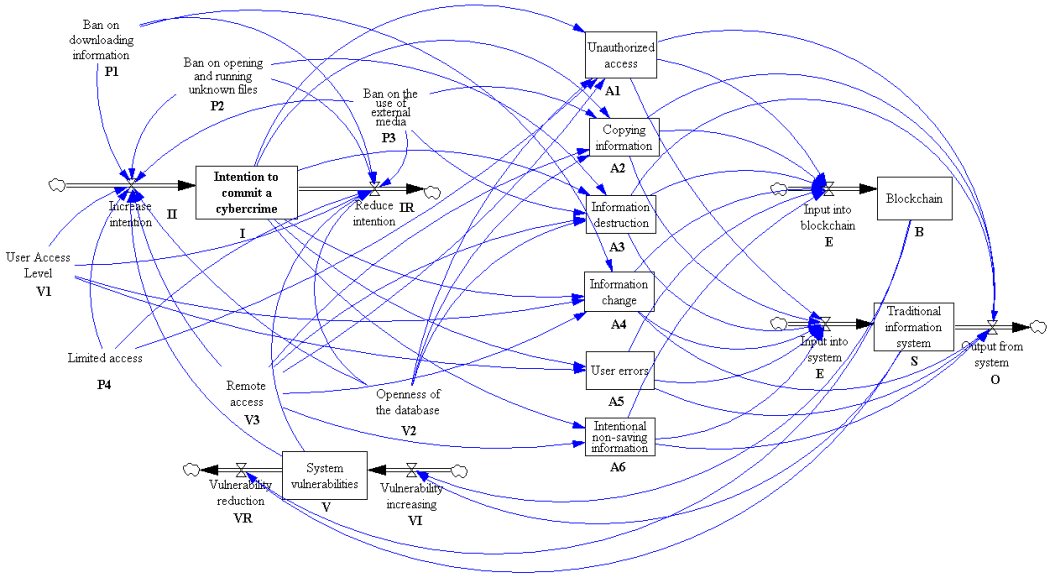

Figure 3. Flow chart
(Source: original development)

$$
\begin{cases}
\dfrac{dI}{dt} = \big(II(t) - IR(t)\big)\,|_{II(t)>IR(t)} \vee \dfrac{dI}{dt} = \big(IR(t) - II(t)\big)\,|_{IR(t)>II(t)} \\
II(t) = \dfrac{1}{1 + EXP\Big(-\big(0.50288 - 2.75474 * (P_1 + P_2 + P_3 + P_4) + 4.8164 * (V(t) + V_1 + V_2 + V_3)\big)\Big)} \\
IR(t) = 1 - II(t) \\
A_1(t) = 1\,|_{V_2 \geq 0.5 \,\vee\, V_3 \geq 0.5 \,\vee\, P_4 < 0.5 \,\vee\, I(t) \geq 0.5} \vee A_1(t) = 0\,|_{V_2 < 0.5 \,\vee\, V_3 < 0.5 \,\vee\, P_4 \geq 0.5 \,\vee\, I(t) < 0.5} \\
A_2(t) = 1\,|_{P_3 < 0.5 \,\vee\, V_2 \geq 0.5 \,\vee\, V_3 \geq 0.5 \,\vee\, I(t) \geq 0.5} \vee A_2(t) = 0\,|_{P_3 \geq 0.5 \,\vee\, V_2 < 0.5 \,\vee\, V_3 < 0.5 \,\vee\, I(t) < 0.5} \\
A_3(t) = 1\,|_{P_2 < 0.5 \,\vee\, P_3 < 0.5 \,\vee\, V_2 \geq 0.5 \,\vee\, V_3 \geq 0.5 \,\vee\, I(t) \geq 0.5} \vee A_3(t) = 0\,|_{P_2 \geq 0.5 \,\vee\, P_3 \geq 0.5 \,\vee\, V_2 < 0.5 \,\vee\, V_3 < 0.5 \,\vee\, I(t) < 0.5} \\
A_4(t) = 1\,|_{P_1 < 0.5 \,\vee\, V_1 \geq 0.5 \,\vee\, V_3 \geq 0.5 \,\vee\, I(t) \geq 0.5} \vee A_4(t) = 0\,|_{P_1 \geq 0.5 \,\vee\, V_1 < 0.5 \,\vee\, V_3 < 0.5 \,\vee\, I(t) < 0.5} \\
A_5(t) = 1\,|_{I(t) \geq 0.5 \,\vee\, V_1 \geq 0.5} \vee A_5(t) = 0\,|_{I(t) < 0.5 \,\vee\, V_1 < 0.5} \\
A_6(t) = 1\,|_{I(t) \geq 0.5 \,\vee\, V_3 \geq 0.5} \vee A_6(t) = 0\,|_{I(t) < 0.5 \,\vee\, V_3 < 0.5} \\
E(t) = A_1(t) + A_2(t) + A_3(t) + A_4(t) + A_5(t) + A_6(t) \\
\dfrac{dB}{dt} = \left(\dfrac{1}{2} + \dfrac{1}{2} * \left[\dfrac{1}{6} * E(t)\right]|_{E(t) \geq 2}\right)|_{E(t) \geq 1} \vee \dfrac{dB}{dt} = 0\,|_{E(t) < 1} \\
O(t) = A_1(t) + 4 * A_2(t) + 2 * A_3(t) + 3 * A_4(t) + 5 * A_5(t) + 6 * A_6(t) \\
\dfrac{dS}{dt} = \left(\dfrac{1}{4} + \dfrac{1}{4} * \left[\dfrac{1}{6} * O(t)\right]|_{E(t) \geq 2}\right)|_{E(t) \geq 1} \vee \dfrac{dS}{dt} = 0\,|_{E(t) < 1} \\
\dfrac{dV}{dt} = \big(VI(t) - VR(t)\big)\,|_{VI(t)>VR(t)} \vee \dfrac{dV}{dt} = \big(VR(t) - VI(t)\big)\,|_{VR(t)>VI(t)} \\
VI(t) = 1\,|_{B(t)>0.5 \,\vee\, S(t)>0.5} \vee VI(t) = 0\,|_{B(t) \leq 0.5 \,\vee\, S(t) \leq 0.5} \\
VR(t) = 1\,|_{B(t) \leq 0.5 \,\vee\, S(t) \leq 0.5} \vee VR(t) = 0\,|_{B(t)>0.5 \,\vee\, S(t)>0.5} \\
P_1, P_2, P_3, P_4, V_1, V_2, V_3 \in [0,1]
\end{cases}
\tag{1}
$$

The flow diagram allowed the simulation to be performed. For this purpose, the values of the initial parameters were changed and their 128 combinations of limit values were taken. The values for the parameters (a ban on downloading information, a ban on opening and running unknown files, a ban on the use of external media, restricted access) were equal to 1 if there are bans and restrictions in the company, or 0 if there are none. The value for user access level, database openness, and remote access was 1 if these parameters are typical for the system, and 0 if these parameters are missing. The simulation occurred at the same time interval. As a result, 128 cases of system behavior were collected for using blockchain technologies and a traditional information system. The result of the simulation is shown in Figure 4.

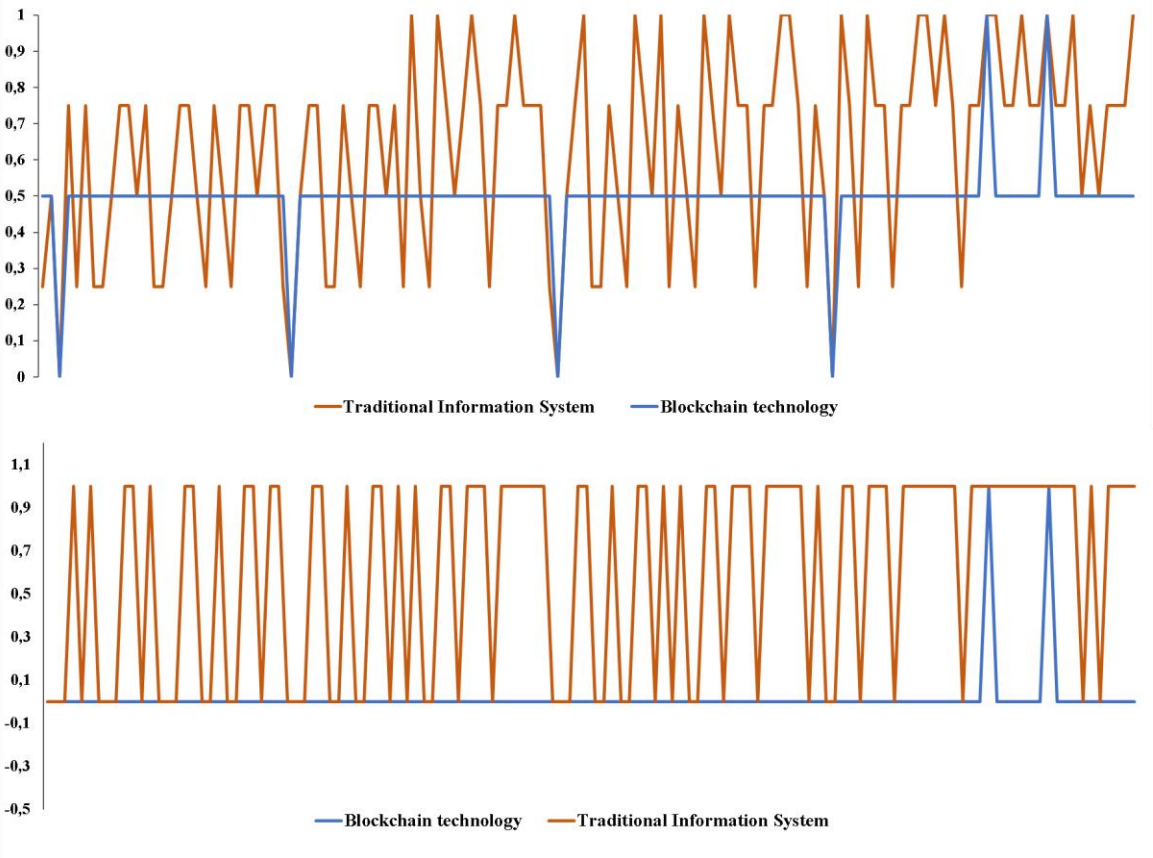

Figure 4: Results of simulation
(Source: original development)

The upper graph of Figure 4 shows the level of risk that is determined by a system that uses blockchain technology and a traditional information system. According to the implemented method, if the value approaches 0, the risk of not detecting cybercrime activity is lower; if the value approaches 1, the risk is higher. Thus, in almost all cases, a system using blockchain technology has a lower risk level than a traditional information system. The cases where both systems have a risk level equal to 1 are cases where the company does not establish a ban, provides unlimited access to users, i.e. this is an option when all security measures are missing. Accordingly, in this case, no technology can positively affect the cyber security system. The lower graph in Figure 4 shows the impact of the identified data on system vulnerabilities. A value of 0 indicates a decrease in vulnerabilities, and 1 indicates an increase in vulnerabilities. In other words, the use of blockchain technology will reduce the vulnerability of the system in almost most cases, and the use of a traditional information system only in some cases. As a conclusion, the use of blockchain technology is more effective than traditional databases, which will positively affect the reliability of the company's cyber security system.

5. CONCLUSION

Thus, the problems associated with the violation of the reliability of cybersecurity systems are relevant. The consequences may be the loss of financial resources, customer trust, and reduced reputation and competitiveness. Therefore, cyber security experts must respond in a timely manner in the event of new types of cyber threats or an increase in the likelihood of vulnerabilities in the system. There are no unique tools that can fully solve cyber security problems. Thus, it should be a set of measures that will contribute to the effectiveness and reliability of the defense system. Most companies increase their investment in the use of modern technologies, which is condemned by some experts. In our opinion, this is the right approach, because the increase in the volume of information, the level of human awareness in the use of modern technologies and devices require new and non-standard approaches. The blockchain technology is being increasingly used and its scope of application is expanding. Therefore, there is a fairly good prospect of using it to increase the level of reliability of the cyber security system in enterprises. The system-dynamic modeling allows making assumptions about the advantages of this technology over traditional information systems. First, this technology will not replace the existing one but will complement it, since its main prerogative is to store information in its original form without changes, which will allow detecting deviations when trying to implement changes. In the future, it is planned to expand the proposed model by taking into account other parameters: to increase the number of activities, especially by external users; to take into account the impact factors at the level of recording data in the blockchain and in the traditional database.

ACKNOWLEDGEMENT: *The research was supported by the Ministry of Education and Science of Ukraine and performed the results of the project "Cybersecurity in the banking frauds enforcement: protection of financial service consumers and the financial and economic security growth in Ukraine" (registration number 0118U003574).*

LITERATURE:

1. Berzin, P., Shyshkina, O., Kuzmenko, O., Yarovenko, H. (2018). Innovations in the Risk Management of the Business Activity of Economic Agents. *Marketing and Management of Innovations, 4,* 221-233. doi: http://doi.org/10.21272/mmi.2018.4-20
2. Bilan, Y., Brychko, M., Buriak, A., Vasilyeva, T. (2019a). Financial, business and trust cycles: The issues of synchronization | [Ciklusi financiranja, poslovanja i povjerenja: pitanja za sinkronizaciju]. *Zbornik Radova Ekonomskog Fakultet au Rijeci, 37*(1), 113-138. doi: http://doi.org/10.18045/zbefri.2019.1.113
3. Bilan, Y., Đšuzmenko, Đž., Boiko, A. (2019b). Research on the impact of industry 4.0 on entrepreneurship in various countries worldwide. *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020,* 2373-2384. Retrieved 30.04.2020 of from https:// ibima.org/accepted-paper/research-on-the-impact-of-industry-4-0-on-entrepreneurship-in-various-countries-worldwide.
4. Bilan, Y., Rubanov, P., Vasylieva, T., Lyeonov, S. (2019c). The influence of industry 4.0 on financial services: Determinants of alternative finance development | [Wpływ przemysłu 4.0 na usługi finansowe: determinanty rozwoju alternatywnych finansów]. *Polish Journal of Management Studies, 19*(1), 70-93. doi: 10.17512/ pjms.2019.19.1.06
5. Boiarko, I., Samusevych, Y. (2011). Role of intangible assets in company's value creation. *Actual Problems of Economics, 3*(117), 86-94. Retrieved 30.04.2020 of from https:// www.researchgate.net/publication/292366060_Role_of_intangible_assets_in_company's _value_creation.

6. CBINSIGHTS. (2020). *Banking Is Only The Beginning: 58 Big Industries Blockchain Could Transform.* Retrieved 01.05.2020 from https://www.cbinsights.com/research/ industries-disrupted-blockchain.
7. Choo, K.-K.R., Dehghantanha, A., Reza M. Parizi, R.M. (Editors). (2020). *Blockchain Cybersecurity, Trust and Privacy.* Springer. vi, 290. https://doi.org/10.1007/978-3-030-38181-3
8. Cosmulese, C.G., Grosu, V, Hlaciuc, E., Zhavoronok, A. (2019). The Influences of the Digital Revolution on the Educational System of the EU Countries. *Marketing and Management of Innovations, 3,* 242-254. doi: http://doi.org/10.21272/mmi.2019.3-18
9. DELLTechnologies. (2020). *Data Protection in a Multi-Cloud World.* Retrieved 01.05.2020 from https://www.dellemc.com/lv-lv/collaterals/unauth/infographic/products/ data-protection/global-data-protection-index-2020-snapshot.pdf.
10. Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps.* Apress. xv, 255. doi; 10.1007/978-1-4842-2604-9
11. Druhov, O., Druhova, V., Pakhnenko, O. (2019). The influence of financial innovations on eu countries banking systems development. *Marketing and Management of Innovations, 3,* 167-177. doi: http://doi.org/10.21272/mmi.2019.3-13
12. EY. (2018). *Cybersecurity: more than protection? EY International Information Security Survey 2018-2019.* Retrieved 01.05.2020 from https://www.ey.com/Publication/vwLU Assets/ey-global-information-security-survey-rus/$FILE/ey-global-information-security-survey-rus.pdf.
13. Grenčíková, A., Bilan, Y., Samusevych, Y., Vysochyna, A. (2019). Drivers and Inhibitors of Entrepreneurship Development in Central and Eastern European Countries. *Proceedings of the 33rd International Business Information Management Association Conference, IBIMA 2019: Education Excellence and Innovation Management through Vision 2020,* 2536-2547. Retrieved 30.04.2020 from https://ibima.org/accepted-paper/ drivers-and-inhibitors-of-entrepreneurship-development-in-central-and-eastern-european-countries/
14. Grytsenko, L., Vysochina, A. (2012). Balanced Scorecard as an assessment tool for enterprise strategy. *Actual Problems of Economics, 3,* 161-167.
15. Grytsenko, L., Boyarko, I., Roenko, V. (2010). Controlling of enterprises cash flows. *Actual Problems of Economics, 3,* 148-154.
16. IBM Security. (2020). *X-Force Threat Intelligence Index 2020.* Retrieved 01.05.2020 from https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf.
17. Kendiukhov, I., Tvaronavičienė, M. (2017). Managing innovations in sustainable economic growth. *Marketing and Management of Innovations, 3,* 33-42. doi: http://doi.org/10. 21272/mmi.2017.3-03
18. Korablinova, I.A. (2017). Tendencies and features of development of companies in digital epoch. *Marketing and Management of Innovations, 1,* 289-299. doi: http://doi.org/10. 21272/mmi.2017.1-26
19. Ledger Insights. (2020). *CB Insights says enterprise blockchain funding less than 20% of cryptocurrencies. But is it?.* Retrieved 01.05.2020 from https://www.ledgerinsights.com/ cb-insights-enterprise-blockchain-funding.
20. Leonov, S.V., Vasilyeva, T.A., Shvindina, H.O. 2017. Methodological approach to design the organizational development evaluation system. *Scientific Bulletin of Polissia, 3*(11), 2, 51-56. doi: http://doi.org/10.25140/2410-9576-2017-2-3(11)-51-56
21. Levchenko, V., Boyko, A., Savchenko, T., Bozhenko, V., Humenna, Yu., Pilin, R. (2019). State regulation of the economic security by applying the innovative approach to its assessment. *Marketing and Management of Innovations, 4,* 364-372. doi: http://doi. org/ 10.21272/mmi.2019.4-28

22. Levchenko, V., Kobzieva, T., Boiko, A., Shlapko, T. (2018). Innovations in Assessing the Efficiency of the Instruments for the National Economy De-Shadowing: the State Management Aspect. *Marketing and Management of Innovations, 4,* 361-371. doi: http://doi.org/10.21272/mmi.2018.4-31
23. Lyeonov, S., Kuzmenko, O., Yarovenko, H., Dotsenko, T. (2019). The innovative approach to increasing cybersecurity of transactions through counteraction to money laundering. *Marketing and Management of Innovations, 3,* 308-326. doi: http://doi.org/ 10.21272/mmi.2019.3-24
24. Melnyk, L. (2017). Paradigm modeling studies of the formation of a knowledge economy in the information society. *Marketing and Management of Innovations, 2,* 269-279. doi: http://doi.org/10.21272/mmi.2017.2-25
25. Pakhnenko, O., Liuta, O., Pihul, N. (2018). Methodological approaches to assessment of the efficiency of business entities activity. *Business and Economic Horizons (BEH), 14*(1), 143-151. doi: http://doi.org/10.15208/beh.2018.12
26. Ponemon Institute. (2019). *2019 Cost of a Data Breach Report.* Retrieved 01.05.2020 from https://www.all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost _of_a_ Data_Breach_Report_final.pdf.
27. Rios, R., Lopez, J.B.L., Veiga, J.G. (2018). The fifth global Kondratiev: low economic performance, instability and monopolization in the digital age. *Marketing and Management of Innovations, 2,* 270-291. doi: http://doi.org/10.21272/mmi.2018.2-22
28. Rubanov, P., Vasylieva, T., Lyeonov, S., Pokhylko, S. (2019). Cluster analysis of development of alternative finance models depending on the regional affiliation of countries. *Business and Economic Horizons (BEH), 15*(1), 90-106. doi: http://doi.org/10. 22004/ag.econ.287251.
29. Semenova, K.D., Tarasova, K.I. (2017). Establishment of the new digital world and issues of cyber-risks management. *Marketing and Management of Innovations, 3,* 236-244. doi: http://doi.org/10.21272/mmi.2017.3-22
30. Sotnyk, I., Zavrazhnyi, K., Kasianenko, V., Roubík, H., Sidorov O. (2020). Investment Management of Business Digital Innovations. *Marketing and Management of Innovations, 1,* 95-109. doi: http://doi.org/10.21272/mmi.2020.1-07
31. TADVISER, 2020. *Blockchain. | [Blokcheyn].* Retrieved 01.05.2020 from http://www. tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0% 91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD_(Blockchain)# .D0.9A.D0.B8.D0.B1.D0.B5.D1.80.D0.B1.D0.B5.D0.B7.D0.BE.D0.BF.D0.B0.D1.81.D0. BD.D0.BE.D1.81.D1.82.D1.8C.
32. Tapscott, D., Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. Portfolio / Penguin. 365.
33. Vasylieva, T.A., Leonov, S.V., Kryvych, Ya.N., Buriak, A.V. (2017a). Bank 3.0 concept: global trends and implications. *Financial and credit activity: problems of theory and practice, 1*(22), 4-10. doi: https://doi.org/10.18371/fcaptp.v1i22.107714
34. Vasylieva, T.A., Lieonov, S.V., Petrushenko, Yu.M., Vorontsova, A.S. (2017b). Investments in the system of lifelong education as an effective factor of socio-economic development. *Financial and credit activity: problems of theory and practice, 2*(23), 426-436. doi: https://doi.org/10.18371/fcaptp.v2i23.121202
35. Ventana Systems, Inc. (2015). *Vensim.* Retrieved 01.05.2020 from http://vensim.com.
36. VOSviewer. (2020). *Welcome to VOSviewer.* Retrieved 01.05.2020 from https://www. vosviewer.com.