**Ministry of Education and Science of Ukraine**
Sumy State University
Academic and Research Institute
of Business, Economics and Management

# *SOCIO-ECONOMIC CHALLENGES*

Proceedings
of the International Scientific and Practical Conference

***(Sumy, November 14-15, 2022)***


Sumy
Sumy State University
2022

330.3:005(063)
S62

**Editor-in-Chief**
Prof., Dr. ***Vasilyeva Tetyana***, Director of Academic and Research Institute of Business, Economics and Management, Sumy State University

*Approved by the Academic Council of Sumy State University (protocol № 5, 17 November 2022)*

S62 Socio-Economic Challenges: Proceedings of the International Scientific and Practical Conference, Sumy, November 14–15, 2022 / edited by Prof., Dr. Vasilyeva Tetyana. – Sumy : Sumy State University, 2022. – 183 p.

Proceedings of the International Scientific and Practical Conference "Socio-Economic Challenges" are devoted to finding a systemic solution to multidisciplinary problems in the field of modern development, management, administration of various systems, corporate social responsibility, innovation management in various fields of environmental management.

For scientists, scientists, students, graduate students, representatives of business and public organizations and higher education institutions and a wide range of readers.

330.3:005(063)

# THE PRACTICE OF ORGANIZING A CYBER FRAUD PREVENTION SYSTEM AT THE MACRO LEVEL

***Hanna Yarovenko,*** *D.Sc., Visiting Prfessor of the Informatics Departament, University Carlos III of Madrid, Spain; Associate Professor of the Economic Cybernetics Department, Sumy State University, Ukraine*
***Maryna Rozkova,*** *PhD Student, Sumy State University, Ukraine*

Cyber fraud has become one of the most common crimes in the world. The risks associated with them are assessed by companies as extremely high, and the losses from them can exceed the costs of data security and protection. The development of cryptocurrencies and electronic money circulation led to the emergence of increased risks at the entire macroeconomic level [1]. At the same time, the possibilities of income laundering and the level of shadowing of economies have also increased. Accordingly, states lose income and opportunities for development, investment in the country decreases, and international competition and own profits decrease [2,3]. That is why recently the systems of combating such types of crimes are developing at a very fast pace not only at the levels of specific organizations but also at the levels of the state and international communities.

All counteraction systems are based on regulations introduced in the early 2000s. One of the main acts is the Convention on Cybercrime, which outlines the basic rules of international information exchange and the principles of the country's interaction in the information space [4,5]. The UN Convention on Cybercrime contains the main definitions of cybercriminals, their classification, and the purpose of punishment for them at the international level. All defined acts and documents regulating cyber security are aimed at creating a safe information space, protecting the information structure of countries, and defining the principles of interaction between states. All of them note the great importance of cybercrimes and their impact on the economic system of countries since the level of money laundering and financial losses from them can be different and affect the world at a global level [6].

Developed countries combine a lot of indicators that ensure stability at the macroeconomic level. These indicators include not only purely economic indicators but also social, political, and cultural ones.. That is why they need extensive cybercrime protection systems [7]. Each of the European countries at the legislative level has established methods of combating such types of crimes and relies in its activities on international treaties and acts. The CERT-EU organization is successfully operating in Europe, the main purpose of which is to detect cyber

attacks using special technologies. Then the detected violations are sent to the European Center for the Investigation of Cybercrimes, where they are studied and further punished by the law [8]. Every organization that uses even the smallest technologies has its corporate crime prevention system, which is the most effective in terms of the activity of this or that enterprise. For example, post-Soviet countries such as Armenia, Georgia, and Azerbaijan integrate cyber security systems into innovative technologies immediately after their creation [9]. Nigeria has its anti-crime system, which is integrated into small and medium enterprises and implemented in various areas such as education and banking [10]. Indonesia's defense systems are built on established relationships between people and delegation. The distribution of protection between agents in different areas allows for creating multi-level security of information at different stages of interactions [11].

One of the strongest systems for countering cybercrime is the UK system. In addition to international treaties, it is based on its strong directions of state policy regarding cyber security. Britain was one of the first countries in the world to introduce liability for crimes related to computer technology back in 1981. The main area of protection in Britain is government organizations and state institutions, as well as the protection of personal data of citizens [12]. And the greatest protection, in this case, is the adopted legislative acts, which determine not only administrative but also criminal responsibility for committing cybercrimes. Normative regulation of cyber security is still the main means of combating crime in most countries of the world, and financing and development of technologies for forecasting and detecting possible threats is an auxiliary means.

Recent years have led to the transition of business online. Many companies were forced to implement e-commerce due to the development of the pandemic: some companies moved completely to the online sector, and some increased electronic cash flow [13]. But in every country business has undergone changes. The field of health care has also changed, due to many things it has also gone electronic. Thus, electronic patient offices, electronic declarations, and vaccination certificates were created en masse [14,15]. The flow of user data has increased significantly, accordingly, the risks of information loss have also increased. Therefore, there is a new requirement for state governments to create security systems that will be reliable enough to store this type of data. Developed countries such as Germany, France, the United States of America, and Britain were able to quickly adapt to new conditions and implement protective systems [16]. For Ukraine, the adaptation system also passed quite quickly. The healthcare system has improved significantly, and electronic certificates are recognized internationally. No leakage of patient data was observed, which indicates a high level of information security. Since the beginning of the pandemic, business in Ukraine has also changed significantly and directed its own protection systems to combat cybercrimes[17].

In Ukraine, the number of cyber frauds has also increased significantly recently, which is due to many factors [18]. The first and most important factor at the moment is the war, leaving the digital sphere - the first sphere to be affected long before the full-scale invasion of the Russian Federation began. Thus, since 2014, the country's energy systems, government websites, including the website of the President of Ukraine, the Ministry of Defense, the Ministry of Finance, and the Ministry of Foreign Affairs, as well as the websites of the most famous Ukrainian mass media, have been affected in the process of cyber warfare. In January and early February 2022, attacks by cybercriminals became massive and were aimed at producing information from the internal databases of the Ukrainian government, as well as from the largest banks of Ukraine: Privatbank, Oschadbank, and others. Major attacks caused some sites to stop working or damage them. Mass cyberattacks were also carried out on users of Twitter, Telegram, Facebook, as well as other social networks to gain access to private devices and monitor Ukrainian citizens to facilitate the genocide.

There were phishing attacks on Ukrainian military personnel and their families, as well as on the private addresses of Ukrainians. The stolen information was released or used in mass terror during the invasion. Also, at the end of April 2022, systematic attacks were used on Elon Musk's Starlink system, then they became the main systems for providing access to high-speed Internet for the needs of the army and in those places affected by the Russian occupation.

Most of the attacks did not achieve their full success; after 2014, the Ukrainian system of countering cyber fraud in all areas has seen significant changes and has become more effective.

Until 2014, the concept of cybercrime was not defined in Ukraine. There was no legally approved method of combating them. The basis of protection against cybercrimes was voluntary united IT specialists or specialists of the Security Service of Ukraine in various departments, who exercised control over the technologies necessary for the work of the government. Each private organization, whether financial or social, had its specialists. In the conditions that existed at that time, the defense took place, albeit at a scattered level, but at a sufficient level, and with the beginning of the war, the direction and number of attacks, as already mentioned, increased. Therefore, there was an urgent need to create a new system that could provide Ukrainians with reliable protection. In 2014, the activities of the CERT-UA team, which became the main asset for responding to the emergence of cyber threats, were established at the state level. Among this team were analysts and programmers who identified the possibility of weak points in government systems and used their improvement. Already in 2016, the cyber security strategy of Ukraine was approved, and a special National Cyber Security Coordination Center was created. This center provided a complete set of actions to combat cybercrime. They carried out analytical and preventive activities. The center was able to create programs to counter threats,

provide the financial and technical basis for programs, as well as participate in international programs and training on the implementation of cyber security in the country and gain foreign experience. Thanks to various international funds and defense associations, equipment and software arrived in Ukraine, which made it possible to provide a more effective response to opportunities and existing cyber threats [19].

In 2018, the Security Service of Ukraine opened the Cyber Security Situation Center. The center is equipped with the technical means used by NATO countries, which allows to ensure uninterrupted work of state services and protect the data of Ukrainians even today. Blocking Russian resources and some social networks was another strategy to combat cybercrime, which made it possible to resist the outflow of information about Ukrainian users and protect them from possible espionage and interference in personal life.

The IT Army of Ukraine has become an important factor outside of ensuring the cyber security of the country in the conditions of war. This army, which consists of programmers, analysts, project managers, etc., was created unofficially on February 24, 2022, and became another front for Ukraine. Since the beginning of the large-scale war, Ukrainian specialists have not only repelled several attacks on banking institutions and government websites but also carried out several successful counterattacks on Russian websites, which were the main sources of disinformation. It is worth noting that all joint attacks of Ukrainian and international programmers are not aimed at stealing the data of ordinary citizens or obtaining illegal profits, but at helping in the fight against a war with a neighboring state. That is, they became part of the fight against cyber fraud in modern conditions. In general, the Ukrainian protection system is not perfect. It remains quite scattered and needs a single center of coordination. Also, in Ukraine, there is still no punishment for cybercrimes at the state level for foreign fraudsters, which makes the state vulnerable to attacks from abroad. Ukrainians need international experience to modernize their achievements.

So, it can be noted that the systems of combating cyber fraud in the world are quite developed. Some countries have a legislative basis and include a wide range of powers, functions, and mechanisms. For an effective application, systems must be constantly developed and improved. It is constant progress that will minimize possible risks and create reliable protection.

## References

1. Kibaroğlu, O. (2020). Self Sovereign Digital Identity on the Blockchain: A Discourse Analysis. Financial Markets, Institutions and Risks, 4(2), 65-79. https://doi.org/10.21272/fmir.4(2).65-79.2020.

2. 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. http://doi.org/10.21272/mmi.2018.4-31.

3. Tiutiunyk, I., Zolkover, A., Maslov, V., Vynnychenko, N., Samedova, M., Beshley, Y., & Kovalenko, O. (2020). Indices of innovation activity as components of macroeconomic stability assessment: how does the shadowing of investment flows affect?. Marketing and Management of Innovations, 4, 26-40. http://doi.org/10.21272/mmi.2020.4-02.

4. Tounsi, W. and Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers and Security, 72, 212 – 233. DOI: 10.1016/j.cose.2017.09.001.

5. Naser, N. (2021). Porter Diamond Model and Internationalization of Fintechs. Financial Markets, Institutions and Risks, 5(4), 51-61. https://doi.org/10.21272/fmir.5(4).51-61.2021

6. Skrynnyk, O. (2021). Analysis of Corporate Investment Behaviour in Digital Technologies for Organisational Development Purposes. Financial Markets, Institutions and Risks, 5(3), 79-86. https://doi.org/10.21272/fmir.5(3).79-86.2021.

7. Vysochyna, A., Kryklii, O., Minchenko, M., Aliyeva, A. A., & Demchuk, K. (2020). Country innovative development: impact of shadow economy Marketing and Management of Innovations, 4, 41-49. http://doi.org/10.21272/mmi.2020.4-03

8. Zolkover, A., Renkas, J. (2020). Assessing The Level Of Macroeconomic Stability Of EU Countries. SocioEconomic Challenges, 4(4), 175-182. https://doi.org/10.21272/sec.4(4).175-182.2020

9. Niftiyev, I., Yagublu, N., Akbarli, N. (2021). Exploring The Innovativeness Of The South Caucasus Economies: Main Trends And Factors. SocioEconomic Challenges, 5(4), 122-148. https://doi.org/10.21272/sec.5(4).122-148.2021

10. Umadia K. Sr., Kasztelnik, K. (2020). The Financial Innovative Business Strategies of Small to Medium Scale Enterprises in Developing Country and Influence for the Global Economy Performance. SocioEconomic Challenges, 4(3), 20-32. https://doi.org/10.21272/sec.4(3).20-32.2020

11. Evana, E., Metalia, M., Mirfazli, E., Georgieva, D.V., Sastrodiharjo, I. (2019). Business Ethics in Providing Financial Statements: The Testing of Fraud Pentagon Theory on the Manufacturing Sector in Indonesia. Business Ethics and Leadership, 3(3), 68-77. http://doi.org/10.21272/bel.3(3).68-77.2019.

12. Vasilyeva, T., Kozyriev, V. (2017). Scientific and methodical approaches to determining the center-orientation of financial conglomerates with the factor and cluster analysis. Business Ethics and Leadership, 1(1), 5-15. Doi: 10.21272/bel.2017.1-01

13. Mishenin, Ye., Klisinski, J., Yarova, I., & Rak, A. (2020). Ensuring Healthy Environment: Mechanisms of Cluster Structures Development in the Field of Waste Management. Health Economics and Management Review, 2, 78-90. http://doi.org/10.21272/hem.2020.2-09

14. Oleksich, Zh., Polcyn, J., & Shtorgin, O. (2021). Adaptation of the Best European Practices in Administering Local Health Care Institutions. Health Economics and Management Review, 2, 15-22. http://doi.org/10.21272/hem.2021.2-02.

15. Mamay, A.,Myroshnychenko, Iu., & Dzwigol. H. (2021). Motivation Management Model and Practical Realization Within the Health Care Institutions. Health Economics and Management Review, 2, 23-30. http://doi.org/10.21272/hem.2021.2-03

16. Serpeninova, Yu., Makarenko, I., Plastun, A., Babko, A., & Gasimova, G. (2020). Mapping of the Responsible Investments Instruments in SDG 3 «Good Health and Well-Being» Financing: EU and US experience. Health Economics and Management Review, 1, 106-115. http://doi.org/10.21272/hem.2020.1-10

17. Boronos, V., Zakharkin, O., Zakharkina, L., & Bilous, Y. (2020). The Impact of The Covid-19 Pandemic on Business Activities in Ukraine. Health Economics and Management Review, 1, 76-83. http://doi.org/10.21272/hem.2020.1-07

18. Dawson M. Applying a holistic cybersecurity framework for global IT organizations. Business Information Review. 2018, № 35(2). P. 60–67

19. Cyber security strategy of Ukraine. DOI: http://zakon2.rada.gov.ua/laws/show/96/2016