Journal homepage: https://devma.com.ua/en

DEVELOPMENT MANAGEMENT

UDC 351.72:004.056.5
DOI: 10.57111/devt/4.2023.45

Vol. 22, No. 4. 2023

Issue of Ukrainian financial sector information security

Svitlana Yehorycheva*
Doctor of Economics, Professor
National University "Yuri Kondratyuk Poltava Polytechnic"
36011, 24 Pershotravneva Ave., Poltava, Ukraine
https://orcid.org/0000-0002-7829-7073

Alina Hlushko
PhD in Economics, Associate Professor
National University "Yuri Kondratyuk Poltava Polytechnic"
36011, 24 Pershotravneva Ave., Poltava, Ukraine
https://orcid.org/0000-0002-4086-1513

Yuliia Khudolii
PhD in Economics, Associate Professor
National University "Yuri Kondratyuk Poltava Polytechnic"
36011, 24 Pershotravneva Ave., Poltava, Ukraine
https://orcid.org/0000-0002-6962-3236

Abstract. Protection of financial resources is one of the priority tasks of the state, which determines its independence and subjectivity. This is especially relevant in the case of Ukraine, which is conducting full-scale military operations, therefore the study of the cyber security problem of the financial sphere of Ukraine and the formulation of recommendations for their solution became the purpose of this study. Methods of statistical analysis, systematization and synthesis were used to analyse the dynamics in the field of protection of critical information, whereas the intelligence method, based on open sources, was used to reveal the main trends, methods, and tools of modern cyber fraud. As a result, a list of problems and threats to the financial sector of Ukraine was formed. An assessment of existing trends in the effectiveness of countering such challenges is given, and several recommendations have been developed to prevent the leakage of personal data and the vulnerability of financial structures. Such recommendations included the introduction of clear algorithms for personnel behaviour, separation of subsystems with different levels of access and their restriction of access to external networks, as well as personal digital security rules – use of two-factor authentication, prohibition of transmission of passwords and temporary codes, etc. In the context of the dynamics of the growth of the number of Internet users over the last five years in the world, the international principles of ensuring information security and the legislation of Ukraine, which regulates actions to protect against cyber-attacks, were analysed. The practical significance of the research lies in finding ways to solve problems in the field of information security of the financial sector and forming recommendations that may be useful to the management of financial institutions

Keywords: information security; financial sector; digitalization; threats; cybercrimes; information protection

Article's History: Received: 18.07.2023; Revised: 09.10.2023; Accepted: 29.11.2023

INTRODUCTION

Global digitalisation trends affect all spheres of society – economic, political, security, educational, and everyday life. Information shapes the competitive advantages of not only individual companies but also entire countries. Therefore, this proliferation of technologies conceals countless risks of remote influence on financial processes, which is especially critical for modern Ukraine. Wartime risks only increase the country's responsibility in the

Suggested Citation:
Yehorycheva, S., Hlushko, A., & Khudolii, Yu. (2023). Issue of Ukrainian financial sector information security. *Development Management,* 22(4), 45-52. doi: 10.57111/devt/4.2023.45.

*Corresponding author

area of financial sector information security, being actively studied by the Ukrainian scientific community.

S. Onyshchenko & A. Hlushko (2020), using a systematic approach to the study of information security, formed the structure of such security in the context of the national economy by applying the method of individual system component interconnection. The structural scheme of relations between security elements and the external environment, proposed by the authors, includes such components of threat response as economic sovereignty, which implies the state's control over its resources; protection against external and internal destabilising factors; development of intellectual potential and equivalence of cyber defence systems for finance.

Further discussion on the issue of society digitalisation in times of crisis, S. Onyshchenko *et al.* (2020) and V. Onyshchenko *et al.* (2020) investigated the impact of the COVID-19 pandemic and subsequent quarantine restrictions on the level of technical awareness of society. In the first months of the lockdown alone, the number of new Internet users worldwide increased by 7%, and the development of such areas as virtual work meetings, distance education, and courier delivery has grown exponentially. The authors note that society is immersed in the virtual world, triggered by COVID-19, which has highlighted the security challenges of the information space and forced the global community to reflect on the vulnerability of the system once again. M.O. Kravtsova (2018), focusing on combating cybercrime in Ukraine, identified certain features inherent in such violations of the law and formulated key indicators of their determination – the dynamic development of technical awareness of the population, the introduction of new, more powerful, high-speed information exchange protocols and the objective inertia of law enforcement agencies, which does not allow them to operate proactively.

Modern trends in financial technologies and their impact on the security of banking institutions were studied by Y. Khudolii & L. Svystun (2021). The researchers examined such relevant digital banking tools as mobile wallets, open banking, microservices, artificial intelligence (AI), and blockchain, and noted a gradual change in the business models of Ukrainian banks and their medium-term FinTech development strategies. Although Ukraine is introducing more secure database organisations with a higher degree of reliability, the authors recommend anticipating the growing demand for online services based on the experience of global banking trends. V. Onyshchenko *et al.* (2020) highlighted such vulnerable aspects of the financial system as electronic payment services, the cryptocurrency market, deliberate dissemination of misinformation, etc. The authors insist that the indicators of the country's digitalisation should also be perceived through the prism of growing threats and the need to ensure proper financial security. V. Bozhenko *et al.* (2021) investigated the rapid cyber fraud spread in the financial sector of Ukraine, identified the main initiators of cyberattacks and the specifics of their criminal activities, stating that the most common forms of such illegal actions are hidden mining, ransomware and deception software that distract the security services of financial institutions from the real epicentre of the attack.

As confirmed by the Ukrainian researchers, the financial sector of Ukraine, albeit belatedly, joined the global fight against cybersecurity challenges. As such, the study aims to analyse the current situation in terms of ensuring its information security.

MATERIALS AND METHODS

The study employed statistical analysis of national economic security indicators, such as the number of registered cyber incidents, types of suspicious files detected by the Vulnerability Detection System of the State Service for Special Communications and Information Protection of Ukraine, and the geography of detections of critical information security events in 2022 and 2023. Statistical analysis and available information security indicators were used to formulate forecasts for further data leakage statistics and the development of the situation in the medium term.

An analysis of the remote access technologies' penetration into people's lives and the dynamics of the number of Internet users in the world from 2019 to 2023 was also conducted to determine the extent of the recent intensive growth of the economy's digitalisation caused by the COVID-19 pandemic and forced quarantine restrictions. Furthermore, the development and transformation of malicious tools for influencing the financial system of Ukraine were studied, and the change in capabilities and effectiveness of cyberattacks over the past few years was examined by a comparative method.

In particular, the study tracked the compliance of existing information system security factors with such principles as legality, comprehensiveness, integration with international rules, balance of interests and cost-effectiveness. The materials used in the study include existing criteria for assessing information security, the concept of a target's hacker attack chain, and the European Union Agency for Network and Information Security experience.

Existing information risks in financial activities were summarised and structured using the systematisation method, including the risk of significant financial data leakage, the risk of destruction of such information in the absence of a recently created backup copy, dissemination of false or negative information in the information space, etc. Such risks were further divided by classification into accidental, intentional, and manipulative.

Since the current martial law requires, for security reasons, additional protection of the financial sector and partially restricted access to the relevant state financial information, an Open-Source Intelligence (OSINT) method was used to form a list of key threats of external interference by intruders in the operating system of financial institutions and to provide examples of fraudulent calls received by bank customers. In particular, examples of calls to consumers on behalf of the security service of banks or other financial institutions were given, which highlight the risks of hacking personal accounts in real-time and using the stressful state of customers to acquire their passwords, temporary access codes, etc.

Through the synergistic effect of the application of existing methods, numerous problems of ensuring information security of the financial sector of the national economy of Ukraine were identified and formulated, and by using existing materials and analysing the research results, several recommendations were made to overcome the threats of their cyber vulnerability.

RESULTS

The current level of technology may be used to significantly increase innovative production, speed up communication processes, and accelerate the development and introduction of new financial products in Ukraine using digital tools. However, this development also has an issue: the digitalisation of financial transactions increases their vulnerability to remote influence, which is an additional factor of instability.

According to the official report of the System for Detecting Vulnerabilities and Responding to Cyber Incidents and Cyber Attacks of the State Service for Special Communications and Information Protection of Ukraine, in 2022, monitoring and analysis tools processed about 58 billion events, detected 181 million suspicious cyber events, processed 179,000 critical events, almost 90,000 suspicious unique files, and documented 415 cyber incidents by System analysts (Statistical report..., 2023). Not only are the absolute figures noteworthy, but also the dynamic development of these indicators – in 2022, the relevant Ukrainian services registered almost three times as many cyber incidents as in 2021. At the same time, most of the new attacks were geolocated in Russia, which means that the protection of Ukraine's information space has become another frontline.

According to the results of the first half of 2023, the State Service for Special Communications notes a certain change in the tactics of cybercriminals representing the interests of the aggressor country – a qualitative transition from an onslaught of simple destructive attacks to more intelligent espionage, implantation and downloading of victim-related data (Russian cyber operations, 2023). The number of incidents more than doubled, from an average of 57 per month in 2022 to 128 per month in 2023. At the same time, Ukraine's special information defence services are also improving their skills: the share of critical incidents fell by 80% – from 144 (first half of 2022) to 27 (first half of 2023) and the number of incidents with negative consequences decreased by 48%. This trend suggests that the protection of important information, including that of the financial sector, has improved. As for the general trend of increasing the number of Internet users, the data for several previous years is shown in Figure 1.

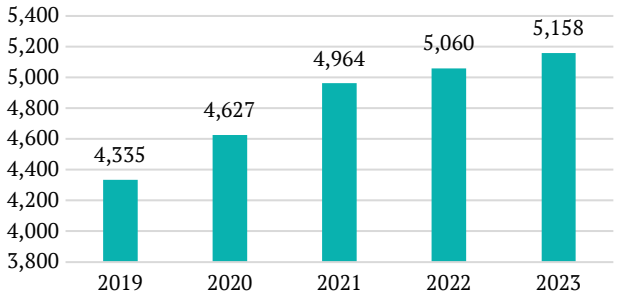

Figure 1. Dynamics of the number of Internet users in the world, billion people

Source: compiled by the authors based on Digital 2023: Global overview report (2023)

Figure 1 shows a rapid increase of almost 14% in the number of Internet users in 2020 and 2021, driven by the need to comply with quarantine requirements and communication limitations. Many banking and financial services customers were forced to discover the benefits of remote account management, making various types of fraud and information manipulation simpler. The principles of ensuring information security include confidentiality, legality, integrity and maintaining a balance between the interests of the state and individuals. There is an international standard of criteria for assessing information security, which is formulated in English as Confidentiality, Integrity, and Availability or, in short, CIA. Another important characteristic of information security is unification, as communication between different national security structures must be identical and mutually integrated, therefore preventing international cybercriminals and fraudsters from exploiting loopholes in the laws of different countries.

An example of such a supranational structure for controlling security in cyberspace is the European Union Agency for Network and Information Security (ENISA), which was established in 2004 and whose functions include the development and implementation of common standards for combating crimes in the virtual environment, the development of an appropriate expert culture, as well as the protection of public and state organisations, enterprises, and individuals within the European Union. In its turn, Ukrainian legislation also attempts to respond to modern security challenges in the information space promptly and ensure the implementation of Article 17 of the Constitution of Ukraine (1996), which provides, in parallel with the protection of Ukraine's sovereignty and state integrity, guarantees of its economic and information security.

In particular, on 14 May 2021, the Decree of the President of Ukraine No. 447 "On Cyber Security Strategy of Ukraine" (2021) was introduced. This Strategy outlines the existing vulnerability of the state's information, economic and financial systems to subversive foreign intelligence services activities in cyberspace and outlines the priorities for appropriate action. These strategic goals include securing cyberspace; sovereignty of the state and the development of society protection; protecting the rights, freedoms, and legitimate interests of Ukrainian citizens in cyberspace; and European and Euro-Atlantic cybersecurity integration. Particular attention should be devoted to The cyber kill chain (2023) concept, which, thanks to Lockheed Martin, moved to the terminology of cyber warfare from "conventional" warfare in 2011 and aims to script a scenario for countering external interference in the information sphere. According to the concept, the chain of countering a hacker attack on a target consists of the following algorithm: detect, shut down, change, corrupt, mislead and deter.

Regarding the problems of ensuring information security in the financial sector, the banking system is the most targeted by criminals, as money is a universal means of payment. In martial law, depriving the enemy of financial resources can significantly reduce the number of available options on the battlefield, and, at last, hacking into financial institutions' databases provides access to the personal data of both individuals and entire organisations. According to the OSINT-acquired data, the key challenges to the information security of financial institutions are gaining access to secret or confidential data; disruption or complete termination of the computer information system;

substitution or deletion of files by intruders; so-called "phishing", when a bank employee clicks on an unfamiliar link and opens access to data on the computer; traffic interception and routing changes.

It is also worth noting that information risks in financial activities can be conditionally divided into accidental, intentional, and manipulative. Accidental risks include the loss of a password (lost media, forgotten password), negligence in creating backups, and physical destruction of servers and databases as a result of a technological failure or natural disaster. Intentional risks include criminal intentions of financial institution employees, hacking of security systems by external intruders, and theft of access media. Manipulative risks are those where fraudsters use deception or blackmail to force bank staff to cooperate, as well as spreading false or negative information in the information space. The total number of cyber incidents in the financial industry, as well as the number of critical financial data leaks worldwide from 2013 to 2022, is visualised in Figure 2.

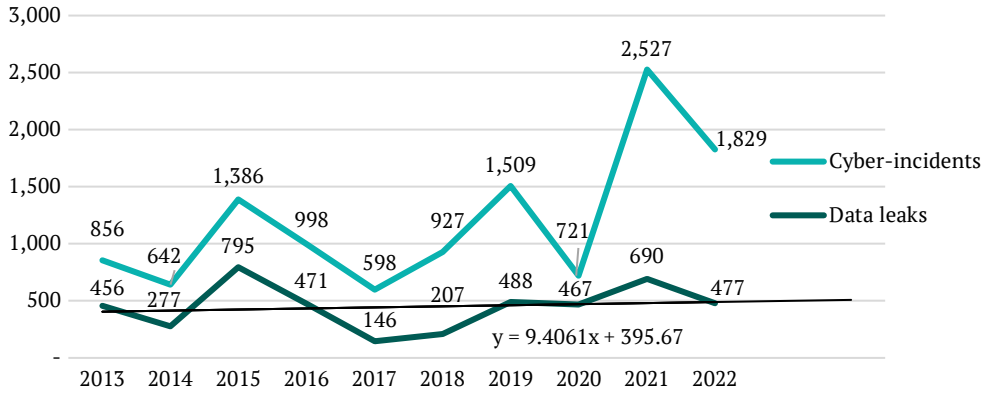

Figure 2. The number of cyber incidents and data breaches in the financial industry worldwide

Source: compiled by the author based on the Number of cyber incidents in the financial industry worldwide from 2013 to 2022 (2023)

According to the data, the number of critical information leaks in the financial sector over the past decade has averaged around 500 events per year. Given the strong technological development that took place between 2013 and 2022 – both in general in various areas of life and the banking sector in particular – this relatively stable figure is rather strange. However, such "passivity" of cybercriminals specialising in data theft might have a rather simple reason. The development of personal data hacking technologies is inseparable from the opposite process – the improvement of the protective mechanisms of financial institutions, and, therefore, the average number of successful attempts does not change critically. As for cyber incidents in general, their number is changing quite dynamically from peaks in 2015, 2019, and 2021 to further declines. As banking institutions change and update their security protocols all the time, this "sine wave" is attributable to various exploits, through which hackers can gain access to financial transactions, as well as the operation of security systems that block identified vulnerabilities – and so on until the next cycle. Therefore, while it is difficult to make detailed forecasts in such an unpredictable industry as cybersecurity, a certain stabilisation of data breach rates in the medium term is notable based on the formation of a trend line.

Numerous information security threats and their diversity require a wide range of countermeasures for financial institution protection. These include, in particular, set algorithms for working with valuable information and the immediate transfer of critical data to an isolated virtual area with minimal and restricted access to the global network. Ideally, a modular data configuration implies a situation in which all subsystems operate separately from each other, and data leakage outside the module is prevented by firewalls. In this case, after preliminary ranking by the degree of importance, the information enters the front office, is transferred for processing to another module, the back office, and then goes for long-term storage in the head office module, which does not have direct access to external Internet networks.

According to several international studies and surveys of banking industry representatives, the human factor is the most vulnerable point of any security system (Villar & Khan, 2021). The lack of digital literacy or negligence among staff causes almost 80% of information security risks (Kurylo *et al.*, 2023). The most illustrative cases include passing passwords to unauthorised or unfamiliar people, disclosing the specifics of the bank's security configuration, following unknown and random links, opening files received from unreliable or unknown addresses, and logging into service subsystems from their unprotected smartphones or laptops.

Therefore, it is worth separating recommendations for overcoming information security problems in financial institutions for employees and individuals, i.e. clients of financial institutions. Staff should undergo frequent and intensive training courses, and understand the existing risks and threats, both old and new. Employees should be obliged to keep proprietary information confidential and non-disclosure, and signed agreements should remain in force even after termination. Each financial institution employee should conduct constant monitoring to detect abnormal situations, unauthorized connections, and unusual activities in the system; regularly back up documents; not use personal computer equipment in a professional environment; regularly change their passwords and in no case keep records at the workplace.

For individuals using bank services, a different list of precautions is used to help protect personal information and funds from fraudsters. There are frequent cases of fraudsters calling from allegedly banking institutions to "prevent illegal debiting of money from the account". Under this fraudulent scenario, financial services consumers, mostly elderly, under the influence of stress and fear of losing their savings, provide confidential information to the criminals, thus opening access to their accounts. A generalised theoretical model of the security system, which is a flowchart showing the interrelationships of various components of the phenomenon, is shown in Figure 3.

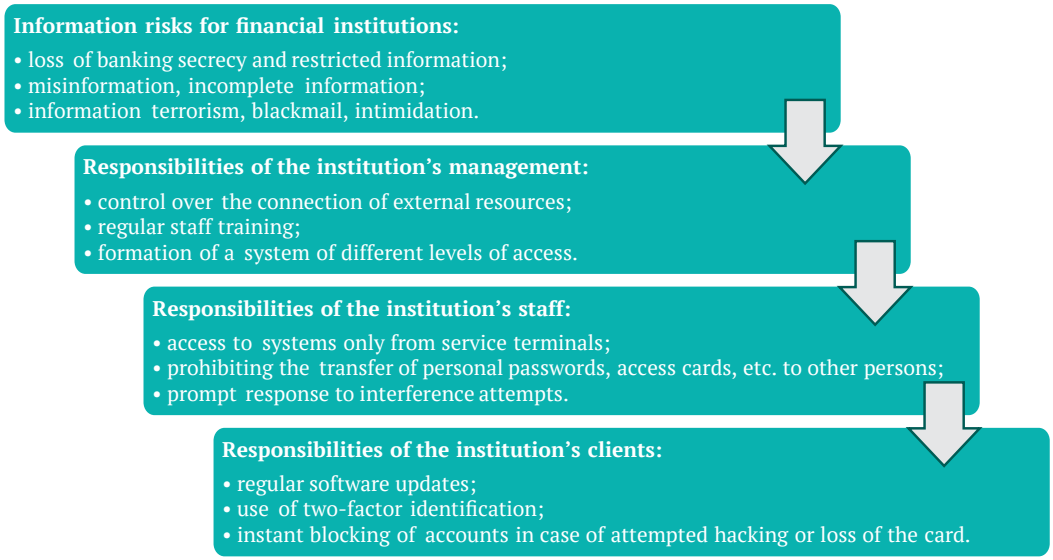

Figure 3. Information security problem-solving model

Source: compiled by the authors

Accordingly, all users of banking services must use two-factor identification, update the bank's software promptly only from official sources, and promptly report fraud attempts. Under no circumstances should passwords, temporary access codes, CVV and PIN codes be disclosed to anyone. Thus, the analysis of the information security challenges faced by financial sector institutions demonstrated, on the one hand, their vulnerability to ever-changing external challenges, and, on the other hand, confirmed that the system's resources are sufficient to respond to and prevent cyber fraud on time.

DISCUSSION

Analysing the study results, it is worth noting the importance of the human factor in security processes and the ability to prevent most cases of cybercrime solely by following existing protocols. It is worth emphasising that the spread and implementation of digital technologies is a global trend. Accordingly, solving information security problems is relevant for the whole world, and many scholars from other countries have also devoted their research to this issue.

S. Calliess & A. Baumgarten (2020), who studied the cybersecurity of the financial sector in the example of the European Union, analysed the existing information protection schemes, their strengths, and weaknesses from a legal point of view, and concluded that the current approach is characterised by the lack of clearly defined areas of responsibility. However, the authors highlight the increasing role of private institutions in shaping the European cybersecurity system and believe that this is a positive practice if such institutions do not have preferences and are governed by a common legal framework. Since in Ukraine, the influence of private entities on the security of the national economy is minimal, this notion may be worth considering (Yesimov & Borovikova, 2023). Methods of detecting credit card fraud in the banking industry were studied by E. Btoush *et al.* (2021). They formulated a thesis, which was confirmed by the author's observations on the growth and diversity of criminal technologies aimed at deceiving consumers of banking services, assessing various techniques, and identifying their advantages and disadvantages. Given the ever-increasing number of bank cards and transactions, the authors compiled a list of recommendations for cardholders to counter this issue more effectively.

The topic of mobile banking, also discussed in this paper, was studied by A. Geebren *et al.* (2021). Considering the issue of mobile applications through the prism of consumer convenience, they noted that trust has a significant positive impact on customer satisfaction. Using partial least squares structural equation modelling, 659 respondents' answers were analysed, determining that trust in the bank and its app is a more important factor in choosing a financial institution than even service quality and profitability. Another perspective on the problem of online banking was presented by A. Sharma *et al.* (2023), who presented their comprehensive empirical research on the security risks of global banking applications. The authors also noted the exponential growth in the number of app users and the risks posed by the massive and dynamic nature of mobile app use and compiled a list of recommendations for users, which, as noted, boils down to the use of two-factor identification and the prohibition of sharing passwords and codes with others.

As cybersecurity risk has emerged as a significant threat to the financial sector, researchers and analysts have sought to understand the issue from different perspectives. M.H. Uddin *et al.* (2020) state that empirical research on this issue based on real data is still limited, but international regulators offer recommendations to combat crime. As noted earlier in this paper, the fight against international crime should be led by supranational bodies, which correlates with the authors' conclusions on the expansion of the powers of such a "cyber-Interpol". S. Varga *et al.* (2021), studying the perception of cyber threats and risk management in the financial sector in the example of Sweden, found that leading participants in the Swedish financial sector already have a well-developed operational concept of regular and crisis management. The survey revealed that much effort is being made to ensure the effective exchange of timely and relevant information between financial institutions, and the importance of communication activities with these institutions was also emphasised in this paper. In general, respondents overwhelmingly agreed that risk management should consider the delay in communications between system units.

To minimise the negative impact of the human factor, which is considered a key threat to the security system, A.S. Villar & N. Khan (2021) conducted a study on the practical use of process robotics in the example of Deutsche Bank. As practice has demonstrated, robotic automation has transformed the financial industry, making popular low-value-added operations much more efficient and allowing banks to improve information security at the same time. H.H. Hettiarachchige & H. Jahankhani (2021) reached similar conclusions, albeit using the UK banking system as an example. They also noted that security and privacy are major concerns for any e-banking system or application and that the transfer of most operations to a remote format creates additional vulnerability, enabling cybercriminals to attack virtual agent endpoints. Nevertheless, the authors' analysis confirmed that the existing two-factor authentication structure meets the requirements for protecting virtual agents in banks.

In terms of the European cybersecurity system in general, S. Fischer-Hübner *et al.* (2021), through 63 interviews with European financial sector professionals, identified key issues in the protection of banking secrecy, as well as challenges and requirements that are to be addressed in the future. As mentioned in this study, an important factor in the cooperation of national economies is the compatibility of protocols for the exchange of confidential information and the joint protection of such communication channels that will prevent fraudsters from manipulating national laws. Hybrid and cyber threats to the European Union's financial system were also the subject of a study by M. Demertzis & G. Wolff (2020). They attempted to achieve a balance between the fragmentation of security systems into separate sub-levels, which were analysed in this paper, and centralisation in financial and other economic matters. The result was a recommendation to EU finance ministers to increase the resilience of the financial and banking systems through regular joint exercises to counter security challenges.

The impact of modern technological capabilities, which have been repeatedly mentioned in this paper, on the transformation of the financial sector was also noted by E. Feyen *et al.* (2021), who noted a significant reduction in transaction costs in the banking sector due to the development of digitalisation. The creation of new business models and the emergence of new financial services market participants inevitably raises several policy issues regarding competition and regulatory spheres of influence that must be agreed upon at the level of national economies. A. Mishra *et al.* (2022), who studied the cybersecurity policies of enterprises in various industries, analysed and compared security protocols governing the implementation of security measures and algorithms for staff behaviour in the event of unusual situations, including cybercrime. Since the importance of strict compliance with such protocols in the banking sector was also emphasised in this paper, it is noteworthy that the results confirmed the same conclusions – cybersecurity requirements in the financial sector are of the highest priority.

The impact of a full-scale war in Ukraine on financial and information security, which was analysed in this paper, was also the subject of research by M. Lehto (2022). The author emphasised that the current security situation on the European continent is the most critical in the previous 80 years and that advanced cyber capabilities are part of a new non-kinetic environment where virtual operations are used in combination with information, financial and electronic warfare. The author analysed the balance between defence and attack in cyberspace and formulates requirements for effective cyber defence. In another paper on the impact of the war on the financial sector, F.M.J. Teichmann *et al.* (2023) note that the operational resilience of financial service providers in Ukraine has deteriorated significantly since the start of full-scale aggression in 2022, but the inherent capacity and assistance of Western financial institutions help the Ukrainian national economy maintain functionality.

In the context of uncertainty and globalisation, it is necessary to consider the impact of financial crises not only on a specific country but also on the global economy. The modern world faces many challenges, but the vulnerability of the financial sector of any country can have the most severe consequences for economic sustainability and development. Comparing the above-mentioned conclusions of the scientific community with the results obtained in this study, it is worth noting a mostly similar assessment of the financial sector's problems and recommendations on how to solve them. Thus, understanding and addressing the problems of the financial sector is an important aspect of global stability and sustainability-based governance.

CONCLUSIONS

Ukraine faces particular risks to the information security of the financial sector, as it is the target of full-scale military operations and the aggressor country's resources for breaching financial security far exceed the capabilities of individual fraudsters or even international criminal organisations. However, the survey results show that both Ukraine and the world have so far managed to successfully counter cyberattacks, demonstrating two tendencies: on the one hand, it is the pursuit of attackers, when certain gaps in information defence are closed in response to their actions, and, on the other hand, proactive actions are taken when potential system exploits are patched beforehand.

The human factor, i.e. staff negligence, remains the weakest and most unpredictable element in the system of financial services, including banking. Risks in this area can be mitigated by constant awareness and responsibility improvement, as employees must understand that approved protocols must be implemented without question and to a word, as even single exceptions can endanger the entire set of protective measures. However, even perfect compliance with the security protocols of financial institution professionals is not enough – each client must, in turn, strengthen collective information security. Customers should protect their personal data and their finances by using only official software and applications, using two-factor authentication, keeping passwords in safe places, and never transferring their cards and qualified electronic signature media to other persons. Since there are no officially recognised state borders for hackers operating remotely, only the same supranational structures with powers that are not burdened by the legislative restrictions of certain states can fight them on an equal footing. The formation of factors for strengthening such international structures to combat cybercrime may be the subject of further research.

ACKNOWLEDGEMENTS

None.

CONFLICT OF INTEREST

None.

REFERENCES

[1] Bozhenko, V., Kushneryov, O., & Kildei, A. (2021). Determinants of spreading cyberthreats in financial sector. *Economic Forum*, 1(4), 116-121. doi: 10.36910/6775-2308-8559-2021-4-16.

[2] Btoush, E., Zhou, X., Gururaian, R., Chan, K., & Tao, X. (2021). A survey on credit card fraud detection techniques in banking industry for cyber security. In *8th international conference on behavioral and social computing (BESC)*. Doha: IEEE. doi: 10.1109/BESC53957.2021.9635559.

[3] Calliess, C., & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: A legal perspective. *German Law Journal*, 21(6), 1149-1179. doi: 10.1017/glj.2020.67.

[4] Constitution of Ukraine. (1996, June). Retrieved from https://www.president.gov.ua/documents/constitution.

[5] Decree of the President of Ukraine No. 447 "On Cyber Security Strategy of Ukraine". (2021, May). Retrieved from https://www.president.gov.ua/documents/4472021-40013.

[6] Demertzis, M., & Wolff, G. (2020). Hybrid and cyber security threats and the EU's financial system. *Journal of Financial Regulation*, 6(2), 306-316. doi: 10.1093/jfr/fjaa006.

[7] Digital 2023: Global overview report. (2023). Retrieved from https://datareportal.com/reports/digital-2023-global-overview-report.

[8] Feyen, E., Frost, J., Gambacorta, L., Natarajan, H., & Saal, M. (2021). Fintech and the digital transformation of financial services: Implications for market structure and public policy. *BIS Papers*, article number 117.

[9] Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., Islami, L., & Akil, M. (2021). Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications*, 61, article number 102916. doi: 10.1016/j.jisa.2021.102916.

[10] Geebren, A., Jabbar, A., & Luo, M. (2021). Examining the role of consumer satisfaction within mobile eco-systems: Evidence from mobile banking services. *Computers in Human Behavior*, 114, article number 106584. doi: 10.1016/j.chb.2020.106584.

[11] Hettiarachchige, H.H., & Jahankhani, H. (2021). Holistic authentication framework for virtual agents; UK banking industry. In R. Montasari, H. Jahankhani, & H. Al-Khateeb (Eds.), *Challenges in the IoT and smart environments* (pp. 245-286). Cham: Springer. doi: 10.1007/978-3-030-87166-6_10.

[12] Khudolii, Y., & Svystun, L. (2021). Modern FinTech trends and their impact on the safety of banking institutions. *Economics and Region*, 3(82), 115-123. doi: 10.26906/EiR.2021.3(82).2375.

[13] Kravtsova, M.O. (2018). Modern status and directions of counteraction of cybercrime in Ukraine. *Bulletin of the Criminological Association of Ukraine*, 2(19), 155-166.

[14] Kurylo, V., Karaman, O., Bader, S., Pochinkova, M., & Stepanenko, V. (2023). Critical thinking as an information security factor in the modern world. *Social and Legal Studios*, 6(3), 67-74. doi: 10.32518/sals3.2023.67.

[15] Lehto, M. (2022). Cyber warfare: The game changer in the battlespace. *Cyberwatch Magazine*, 2022(2), 21-26.

[16] Mishra, A., Alzoubi, Y.I., Gill, A.Q., & Anwar, M.J. (2022). Cybersecurity enterprises policies: A comparative study. *Sensors*, 22(2), article number 538. doi: 10.3390/s22020538.

[17] Number of cyber incidents in the financial industry worldwide from 2013 to 2022. (2023). Retrieved from https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/.

[18] Onyshchenko, S., & Hlushko, A. (2020). Conceptual foundations of information security of national economy in the conditions of digitalization. *Social Economics*, 59, 14-24. doi: 10.26565/2524-2547-2020-59-02.

[19] Onyshchenko, S., Hlushko, A., & Yanko, A. (2020). Role and importance of information security in a pandemic environment. *Economics and Region*, 2(77), 103-108. doi: 10.26906/EiR.2020.2(77).1954.

[20] Onyshchenko, V., Yehorycheva, S., Maslii, O., & Yurkiv, N. (2020). Impact of innovation and digital technologies on the financial security of the state. In V. Onyshchenko, G. Mammadova, S. Sivitska, & A. Gasimov (Eds.), *Proceedings of the 3rd international conference on building innovations* (pp. 749-759). Cham: Springer. doi: 10.1007/978-3-030-85043-2_69.

[21] Russian cyber operations. (2023). Retrieved from https://cip.gov.ua/services/cm/api/attachment/download?id=60201.

[22] Sharma, A., Singh, S.K., Kumar, S., Chhabra, A., & Gupta, S. (2023). Security of android banking mobile apps: Challenges and opportunities. In N. Nedjah, G. Martínez Pérez, & B.B. Gupta (Eds.), *International conference on cyber security, privacy and networking* (pp. 406-416). Cham: Springer. doi: 10.1007/978-3-031-22018-0_39.
[23] Statistical report on the results of the vulnerability detection and cyber incidents/cyber attacks response system operation for 2022. (2023). Retrieved from https://scpc.gov.ua/en/articles/233.
[24] Teichmann, F.M.J., Wittmann, C., & Sergi, B.S. (2023). Operational resilience in light of the war in Ukraine: The disruptive effect of implementing economic sanctions on financial service providers. *Journal of Financial Crime*. doi: 10.1108/JFC-01-2023-0005.
[25] The cyber kill chain. (2023). Retrieved from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.
[26] Uddin, M.H., Ali, M.H., & Hassan, M.K. (2020). Cybersecurity hazards and financial system vulnerability: A synthesis of literature. *Risk Management*, 22, 239-309. doi: 10.1057/s41283-020-00063-2.
[27] Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security*, 105, article number 102239. doi: 10.1016/j.cose.2021.102239.
[28] Villar, A.S., & Khan, N. (2021). Robotic process automation in banking industry: A case study on Deutsche Bank. *Journal of Banking and Financial Technology*, 5, 71-86. doi: 10.1007/s42786-021-00030-9.
[29] Yesimov, S., & Borovikova, V. (2023). Methodological foundations of information security research. *Social and Legal Studios*, 6(1), 49-55. doi: 10.32518/sals1.2023.49.

Проблеми забезпечення інформаційної безпеки фінансового сектору України

Світлана Борисівна Єгоричева

Доктор економічних наук, професор
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
36011, просп. Першотравневий, 24, м. Полтава, Україна
https://orcid.org/0000-0002-7829-7073

Аліна Дмитрівна Глушко

Кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
36011, просп. Першотравневий, 24, м. Полтава, Україна
https://orcid.org/0000-0002-4086-1513

Юлія Сергіївна Худолій

Кандидат економічних наук, доцент
Національний університет «Полтавська політехніка імені Юрія Кондратюка»
36011, просп. Першотравневий, 24, м. Полтава, Україна
https://orcid.org/0000-0002-6962-3236

Анотація. Захист власних фінансових ресурсів – одна з пріоритетних задач держави, що обумовлює її незалежність та суб'єктність. Особливо це актуально у випадку України, що веде повномасштабні воєнні дії, тому вивчення проблеми кібербезпеки фінансової сфери України та формулювання рекомендацій щодо їх вирішення стало метою даного дослідження. Завдяки методам статистичного аналізу, систематизації та синтезу була досліджена динаміка у сфері захисту критично важливої інформації, а за допомогою методу розвідки на основі відкритих джерел виявлено основні тенденції, методи та інструменти сучасного кібершахрайства. В результаті було сформовано перелік проблем та загроз фінансового сектору України. Дана оцінка наявних трендів ефективності протистояння таким викликам, розроблено ряд рекомендацій щодо запобігання витоку особистих даних та уразливості фінансових структур. До таких рекомендацій було віднесено запровадження чітких алгоритмів поведінки персоналу, відокремлення підсистем із різним рівнем доступу та їх обмеження виходу до зовнішніх мереж, а також правила особистої цифрової безпеки: використання двофакторної автентифікації, заборона передачі паролів та тимчасових кодів тощо. У контексті динаміки зростання кількості користувачів Інтернету за 2019-2023 роки у світі було проаналізовано міжнародні принципи забезпечення безпеки інформації та законодавство України, що регламентують дії з захисту від кібератак. Практична значущість дослідження полягає в знаходженні шляхів вирішення проблем у сфері інформаційної безпеки фінансового сектору та формуванні рекомендацій, що можуть бути корисними керівництву фінансових установ

Ключові слова: інформаційна безпека; фінансовий сектор; цифровізація; загрози; кіберзлочини; захист інформації