Business Information Security

Svitlana Onyshchenko, Stanislav Bilko, Alina Yanko, and Svitlana Sivitska

Abstract The article highlights the problem of business information security under digitalization processes spreading, which, being a driver of all the sectors of economy development, at the same time have led to destructive phenomena, namely information wars, information terrorism, large-scale cyber-attacks. Negative impact of the latter, which is seen in huge financial losses, raises the issue of business information security. It is proved that ensuring timely identification of potential and real threats to business information security is necessary in order to minimize and prevent the causes of their manifestation, to develop a set of preventive measures. An information security system is suggested, which is based on a clear algorithm of defined procedures that will ensure reliability, confidentiality, integrity and availability of information resources of the entity, as well as neutralize potential and minimize real risks and threats to the company's information environment, including cyberspace. A number of preventive work approaches to minimize risks to business information security are defined, based on general rules of information security and provide implementation of high-tech strategies for digital protection against cyber threats. The main modern methods of counteracting threats and cyber threats are identified, which allow businesses to identify the possible number of threats, analyze losses, including financial ones, from attacks made, as well as implement preventive measures to minimize risks. Based on the analysis of the annual global financial losses from cyber-attacks and the dynamics of financial investments in cyber security, the need to implement an information security system for each business entity has been proven.

Keywords Digitalization · Information security · Cyber security · Business · Risks · Threats

S. Onyshchenko · S. Bilko · A. Yanko (✉) · S. Sivitska
National University «Yuri Kondratyuk Poltava Polytechnic», Pershotravnevyj Ave 24, Poltava 36011, Ukraine
e-mail: glushk.alina@gmail.com

V. Onyshchenko et al. (eds.), *Proceedings of the 4th International Conference on Building Innovations*, Lecture Notes in Civil Engineering 299,
https://doi.org/10.1007/978-3-031-17385-1_65

1 Business Information Security Under External Challenges and Threats

Hybrid aggression from the Russian Federation has brought up issues of all types of security for citizens, business, and the state, including information security as well. Military invasion is accompanied by war in the information field: information terrorism, large-scale cyber-attacks–these are destructive phenomena that have invaded the modern world. They cause no less damage than direct hostilities. The need to support the national economy during external aggression implies the need to ensure business functioning on the basis of information security.

Problems of business information security, including those in context of supporting financial security of the state are widely relevant in the works of foreign and domestic researchers [1–5]. At the same time, in terms of external aggression, the need to form a security-oriented information environment of business functioning has become especially relevant.

It has to be noted that the problem of business information security, though becoming a priority in the current environment of growing external threats, has become even more relevant since the deepening of digitalization processes.

Undoubtedly, digitalization has become the main development driver for all the spheres of the national economy in the recent years. Technology, smart applications and other innovations in the digital economy have enabled improving the quality and availability of services, solving a number of problems in the areas of health, public administration, education, taxation etc. The COVID-19 pandemic had a significant impact on the deepening [6, 7] of IT technologies use in business processes.

Based on the expert assessments from a number of international organizations, the main advantages that businesses have received in terms of strengthening the digitalization processes, the following can be identified:

(1) Approach to the consumer. In terms of digitalization, the need for intermediaries has significantly decreased. Most companies have developed their own websites, entrepreneurs have opened online stores and have the opportunity to work directly with potential customers;
(2) Cost optimization, which first of all involves reducing marketing costs;
(3) Business processes acceleration, due to reducing the time of communications;
(4) Increasing the efficiency of responding to changes in the market environment;
(5) Increasing the flexibility of the proposed products and their high adaptability to new expectations or the consumer needs [8, 9].

In addition to the positive impact on business development, studies by international organizations also confirm positive effect of digitalization on the level of employment. Thus, according to McKinsey company [10], one new job in the ICT sector stimulates creation of 2–4 additional jobs in the economy as a whole. PWC estimates that a 10% increase in digitalization reduces unemployment by 0.84% [11].

At the same time, rapid development of digitalization processes has become a source of not only new opportunities, but also risks and threats primarily to business information security.

Business information security is a state of information resources and related information tools and systems of the business entity, which guarantees ensuring its activities with the necessary information in a high-quality and uninterrupted way provided a high level of its protection from internal and external threats [12, p. 213].

Accordingly, in terms of deepening the economy digitalization, along with traditional threats to business information security, such as industrial espionage, intentional and unintentional disclosure of confidential information and trade secrets by employees, unfair actions of competitors, including damage to business reputation, interference of third parties in information systems and networks, etc., creates a number of additional threats to information resources and business technologies, methods of diagnosis and counteraction to which have not been fully developed yet [13]. First of all, these are threats related to cyber-attacks, disclosure of personal data, spyware and viruses, phishing, threats connected with updating computer programs etc.

According to official statistics, the level of cybercrime in Ukraine is constantly growing (Fig. 1).

It should be noted that Ukraine ranks second in the world in the number of cyber-attacks, which indicates a low level of protection of the information environment. Thus, according to official Microsoft data, 19% of all cyber-attacks recorded in 2021 were committed against Ukraine (the United States ranking first with 46%). For comparison, the share of Belgium, Germany and Japan does not exceed 3% [15]. At the same time, the main types of cyber-attacks that pose the greatest threat to information security in business are extortionist programs, insider attacks, phishing, targeted cyber-attacks and DDoS attacks.

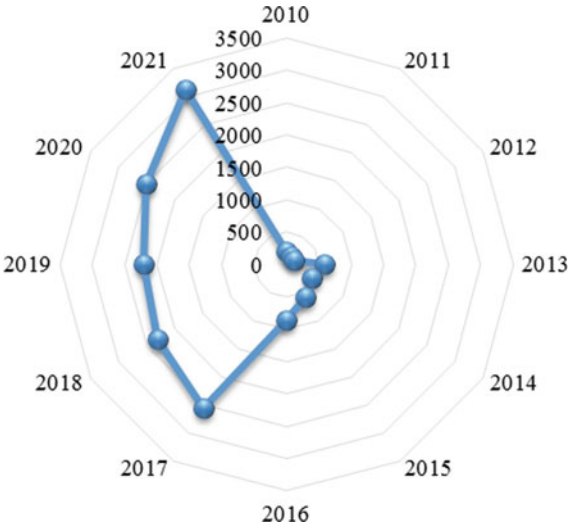

Fig. 1 The level and dynamics of cybercrime in Ukraine in 2010–2021.* Made according to [14]

Extortionist programs or cryptographic programs encrypt information on the company's devices, which can lead to a complete shutdown of business. In some cases, information cannot be recovered.

Insider attacks are one of the most complex types of cyber threats because they are directly related to the human factor. An insider is usually an employee of the company, who causes damage both intentionally and accidentally. This type of cyber-attack is difficult to predict.

Phishing is one of the most common and effective attacks. It is observed when a cyber-attacker emails malicious files or links that infect PCs when opened. This is where the penetration into the organization's network begins.

Targeted cyber-attacks, DDoS attacks, are attacks on a computer system aiming to bring it to failure. They create conditions under which system users cannot access provided system resources or they get limited significantly.

The latter type of cyber-attacks is often used by the Russian aggressor to cover up destructive actions. In particular, the last large-scale and long-lasting DDoS attack on Ukrainian banks and government websites was carried out on February 15, 2022. According to official data, no data leakage, distortion or destruction of elements of the IT infrastructure or financial losses were recorded [16].

These types of threats to information security of business cause the greatest financial losses and, of course, affect the level of financial security of the country as a whole.

In 2020, the losses of the world economy as a result of cyber-attacks amounted to more than 1 trillion US dollars, which was 1% of the world GDP. Compared to 2018, this figure increased by more than 50%. According to official McAfee data, only 4% of the companies surveyed did not face cyber-attacks in 2021. The rest, 96% of companies, have been victims of cyber-attacks to one degree or another. After all, even without suffering direct financial losses from cybercrime, the companies faced with their negative impact on employee productivity, distribution of working time, the image of the company as a whole. The most dangerous for business are cyber-attacks aimed at stealing intellectual property and cyber espionage, which are often accompanied by ransom demands. Nearly 2/3 of all material damage from cyber-attacks is related to financial crimes and loss of intellectual property [17].

Given the above, there is a need to justify a system of business information security that can predict the likelihood, neutralize potential risks and threats to the company's information environment, including cyberspace, and minimize real ones.

2 System of Business Information Security

Taking into account sustainable growth of external and internal threats to business information security and increase of financial losses in case of their occurrence, the issue of the development of the efficient information security system has gained its relevance and topicality for business owners and managers. The system of business information security should be presented as follows (Fig. 2).

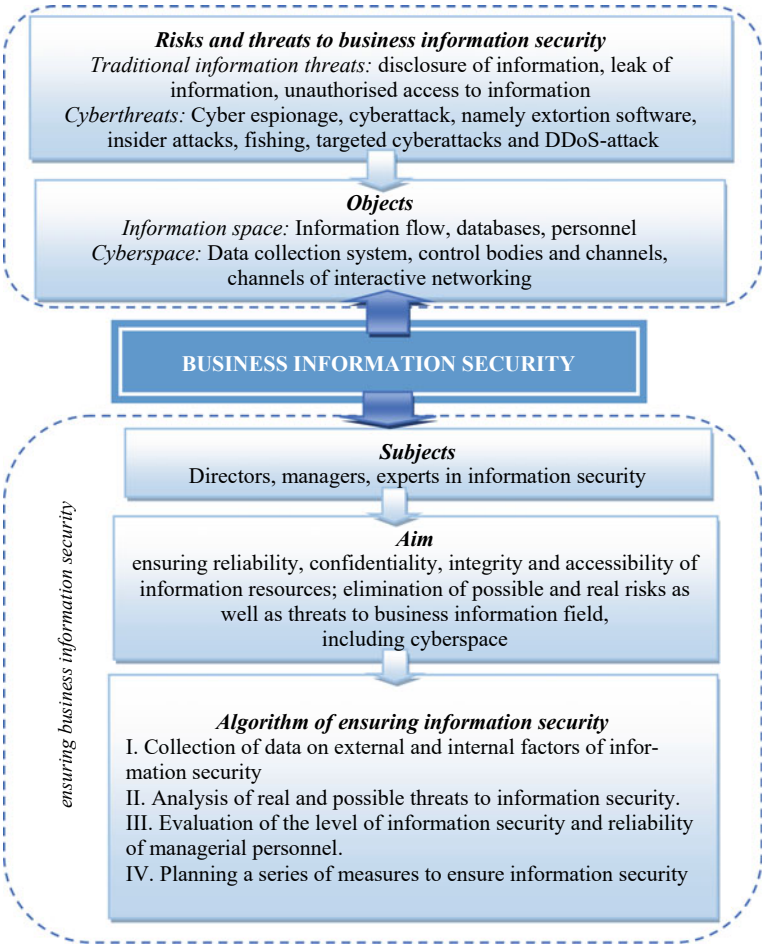

Fig. 2 System of business information security

It should be noted that making a system of business information security should be based on international standards, including ISO/IEC 27,001 and ISO/IEC 27,002, that represent management system model which defines general process organization, data classification, access system, planning directions, staff responsibility, use of risk evaluation, etc. in the context of information security. ISO/IEC 27,001 Standard provides economic entities with the possibilities to evaluate risks, implement the means of control to mitigate them, monitor risks and improve information security if necessary. ISO/IEC 27,002 Standard is used to set up the system of efficient information security and improvement of information security methods [18].

The system of business information security should be based on the clear algorithm of set procedures, which allow ensuring reliability, confidentiality, integrity and accessibility of economic entity's information resources as well as eliminating

possible and minimizing real risks and threats to business information field [19], including its cyberspace. Business owners should consider the fact that promptly and reliably identified risks of business information security, including cyber risks, allows forecasting their impact, foreseeing the probability of their occurrence, developing relevant preventive measures.

A number of approaches to risks prevention concerning business information security is singled out nowadays. The main of them include the following.

'Avoid' (get away from risk) provides for the optimization of business processes through the exclusion from their use of the information whose loss may be critical for the business. So if the firm is not able to provide customers' personal data security, its operation should be arranged without the collection of them.

'Except' as an approach lies in the conscious risk taking without changing business processes, since the latter appears to be more costly than the risk itself. It is appropriate in case of low risk impact on the business.

'Mitigation' means the reduction of risk impact on business. Its implementation is possible with the help of regular monitoring and identification of It-architecture vulnerability to hackers. The sufficiency level of business information security is evaluated according to the monitoring results. If it is insufficient, the business should get insured. In case of business loss, the insurance funds will help e.g., pay fines and cover expenses on the business process resumption. Apart from the aforementioned mechanisms, economic entity can implement the development of additional security elements by the security engineers. They will analyze the threat models, emergencies, etc. and determine the requirements to be used by the developers. After that, the security system can be also tested through its presentation for public hacking aimed at its vulnerability verification by independent 'experts' [20, 21].

After the introduction of measures to prevent business information security risks, it is advisable for management to systematize those threats that are the most real, assess the level of information security and the reliability of management personnel. Based on the results obtained, strategic and operational measures to ensure information security have been developed.

Measures to counter threats to business information security should be based on general information security rules and provide for the introduction of high-tech digital security strategies against cyber threats. In particular, the main areas of countering threats and cyber threats to the safe functioning of a business can be defined as:

- Creation of backup copies of key files to minimize damage from ransom ware attacks;
- Installation and regular updating of security software to counteract known digital threats;
- Regular scanning of all devices connected to the corporate network and prohibition of the use of unverified portable devices;
- Conducting regular trainings and courses for employees in order to teach them the basic rules of cyber security;
- Control of access to accounts and databases;

– Conducting regular security testing of corporate products by conducting penetration tests and participation in bug bounty programs [20].

It is worth noting that the most effective methods of ensuring protection of a business from cyber-attacks are periodic penetration tests and the use of bug bounty programs. In particular, penetration tests enable assessing the degree of access ease to characteristics and data of a company's information system, determining the possible number of threats, analyzing business losses, including financial ones, from implemented attacks, and also implementing preventive measures to minimize risks. In terms of content, penetration tests or penetration test (pen test) are a simulation of a cyber-attack on information systems in order to check their security.

As for bug bounty programs, they are based on the involvement of independent IT specialists (the so-called "moral hackers") in order to identify vulnerabilities in the company's web resources. Performers–ethical hackers–receive a financial reward from the customer, the amount of which depends on the type of problem identified and its scale.

Of course, effective information security system implementation requires significant capital investments from the business. At the same time, investing in information and cyber security is rightfully defined as one of the most effective strategies for preventing financial losses. In addition, a company that is not tainted by cases of loss of data or customer funds is considered a reliable partner and has the opportunity to increase its potential income [22]. Therefore, investment of companies into creation of an effective information security system is an effective way to adapt business to conditions of external environment variability. To confirm this thesis, it is advisable to make a comparison between the level of financial investment in cyber security and financial losses as a result of cyber-attacks, although the real scale of the latter is almost impossible to determine (Fig. 3).

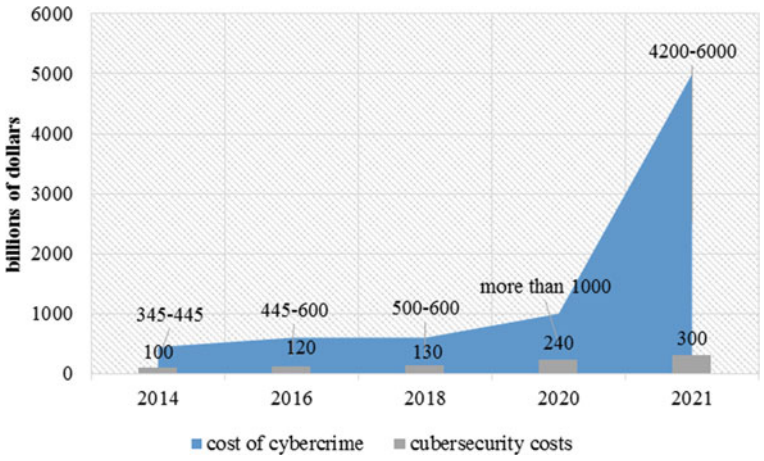

Fig. 3 Estimated average cost of cybercrime and cubersecurity costs

Based on the presented info graphics, built on the official data of research Cyber security Ventures [23], it is legitimate to note the insufficient level of financial investment in cyber security as a component of information security. Over the past five years, from 2017 to 2021, their total volume amounted to 1 trillion USD USA. While the losses from cyber-attacks in 2020 alone amounted to more than this sum, and in 2021 increased to 4.2–6 trillion USD USA. According to experts, in 2025 the amount of financial losses from cybercrime will reach 10.5 trillion USD USA. Regarding the financing of cyber security measures, its growth is projected at 10–15% in the next 5 years.

Thus, considering the results of the study, it is necessary to state the need to build an effective system of information business security. After all, the losses from crimes in the information and cyberspace are much higher than the financial investments that are appropriate in the implementation of security systems in the enterprise [24, 25]. At the same time, business owners have the opportunity to choose the method of organizing the information security system–from the creation of a security service at the company to the use of specialized companies services.

3 Conclusion

In the course of the research it is substantiated that the spread of digitization processes along with the undeniable benefits for the development of both the world and national economies, has led to the emergence of such destructive phenomena as information warfare, information terrorism, cyber-attacks and more. In today's world, information is the most valuable business asset of most companies. In this regard, there is an urgent need to form a security-oriented information business environment, ensuring information business security.

Taking into account the growth of external and internal threats to business information security, increasing the level of financial losses in case of their implementation, a system of business information security is suggested, which is based on a clear algorithm of defined procedures that will ensure the reliability, confidentiality, integrity and availability of the entity information resources, as well as neutralize potential and minimize real risks and threats to the company's environment, including cyberspace. A number of approaches to preventive work to minimize risks to information business security are outlined and the main modern methods of counteracting threats and cyber threats are identified.

The expediency of financial investments in the creation of an effective information security system, which is an effective direction of business adaptation to the changing environment, increase resilience to external risks and threats, are proved.

References

1. Antonyuk V Mechanisms of state response to modern challenges and threats to information security. Homepage. http://www.dy.nayka.com.ua/?op=1&z=747
2. Baranov O (2014) On the interpretation and definition of "cybersecurity." Inform Law 2(42):54–62
3. Lytvynenko O (2017) Information component in the modern hybrid war against Ukraine: challenges and threats. Ukrain Stud Almanac Issue 19:171–174
4. Yarovenko H (2020) Evaluating the threat to national information security. Probl Perspect Manag 18(3):195–210
5. Glushko AD (2013) Directions of efficiency of state regulatory policy in Ukrain. World Appl Sci J Pakistan Int Dig Organ Sci Inform 27(4):448–453. https://doi.org/10.5829/idosi.wasj.2013.27.04.13656
6. Onyshchenko S, Hlushko A, Yanko A (2020) Role and importance of information security in a pandemic environment. Econ Reg 2(77):103–108. https://doi.org/10.26906/EiR.2020.2(77).1954
7. Bilko S (2021) Institutional support of information security of Ukraine. Econ Reg 3(82):36–41. https://doi.org/10.26906/EiR.2021.3(82).2361
8. OECD Digital Economy Outlook 2020. Homepage. https://www.oecd.org/digital/oecd-digital-economy-outlook-2020-bb167041-en.htm
9. Pischulina O (2020) Digital economy: trends, risks and social determinants: report. Tsentr Razumkova. Homepage. https://razumkov.org.ua/uploads/article/2020_digitalization.pdf
10. Manyika J, Lund S, Bughin J, Woetzel J, Stamenov K, Dhingra D (2016) Digital globalization: the new era of global flows. McKinsey & Company. Homepage. http://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows
11. Booz & Company (2012) Maximizing the impact of digitization. Homepage. https://www.strategyand.pwc.com/m1/en/reports/maximizing-the-impact-of-digitization.pdf
12. CIS Controls Implementation Guide for SMEs. Homepage: CIS-Controls-Guide-for-SMEs.pdf (cisecurity.org)
13. Onyshchenko S, Hlushko A, Maslii O, Skryl V (2020) Risks and threats to economic security of enterprises in the construction industry under pandemic conditions. In: Onyshchenko V, Mammadova G, Sivitska S, Gasimov A (eds) Proceedings of the 3rd international conference on building innovations. ICBI 2020. Lecture notes in civil engineering, vol. 181. Springer, Cham, pp 711–724. https://doi.org/10.1007/978-3-030-85043-2_66
14. Official site the cyberpolice department of Ukraine. Homepage. https://cyberpolice.gov.ua/
15. Microsoft Digital Defense Report (2021) Homepage. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
16. Official site the State Service for Special Communications and Information Protection of Ukraine (2022) Ukraine has successfully repulsed the largest DDoS attack in its history. Homepage. https://cip.gov.ua/ua/news/ukrayina-uspishno-vidbila-naibilshu-ddos-ataku-v-svoyii-istoriyi
17. Economic Impact of Cybercrime–No Slowing Down (2018) Report of the Center for Strategic and International Studies (CSIS). Homepage. https://www.csis.org/analysis/economic-impact-cybercrime
18. Onyshchenko, S., Yanko, A., Hlushko, A., Sivitska, S. Increasing Information Protection in the Information Security Management System of the Enterprise. In: Onyshchenko V., Mammadova G., Sivitska S., Gasimov A. (eds) Proceedings of the 3rd International Conference on Building Innovations. ICBI 2020. Lecture Notes in Civil Engineering. Springer, Cham. Volume 181, 725–738 (2020). https://doi.org/10.1007/978-3-030-85043-2_67
19. Glushko A, Marchyshynets O (2018) Institutional provision of the state regulatory policy in Ukraine. J Adv Res Law Econ ASERS Publishing House 9(3):941–948. https://doi.org/10.14505/jarle.v93(33).18.

20. European Business Association (2021) Cybersecurity secrets: rational investment in cybersecurity? Homepage. https://eba.com.ua/sekrety-kiberbezpeky-ratsionalnist-investytsij-u-kiberbezpeku/
21. Svistun L, Glushko A, Shtepenko K (2018) Organizational aspects of investment and construction projects implementation at the real estate market in Ukraine. Int J Eng Technol 7(3.2):447–452. https://doi.org/10.14419/ijet.v7i3.2.14569
22. Onyshchenko SV, Matkovskyi AV, Puhach AA (2014) Analysis of threats to economic security of ukraine in conditions of innovative economic development. Econ Ann-XXI 1–2(2):8–11
23. Morgan S Special report: cyberwarfare in the C-suite. Homepage. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
24. Dzwigol H, Shcherbak S, Semikina M, Vinichenko O, Vasiuta V (2019) Formation of strategic change management system at an enterprise. Acad Strat Manag J 18(1):1–8
25. Onyshchenko V, Yehorycheva S, Maslii O, Yurkiv N (2020) impact of innovation and digital technologies on the financial security of the state. In: Onyshchenko V, Mammadova G, Sivitska S, Gasimov A (eds) Proceedings of the 3rd international conference on building innovations. ICBI 2020. Lecture notes in civil engineering, vol 181. Springer, Cham, pp 749–759. https://doi.org/10.1007/978%2D3%2D030%2D85043%2D2_69