DOI: https://doi.org/10.32782/2524-0072/2022-43-8

УДК 65.012

ХАРАКТЕРИСТИКА ОСНОВНИХ ПРОБЛЕМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ВПЛИВУ ЦИФРОВИХ ТЕХНОЛОГІЙ

THE CHARACTERISTIC OF MAIN PROBLEMS OF PROVIDING INFORMATION SECURITY UNDER THE INFLUENCE OF DIGITAL TECHNOLOGIES

Леськів Галина Зіновіївна
кандидат технічних наук, доцент,
Львівський державний університет внутрішніх справ
ORCID: https://orcid.org/0000-0002-4900-9466

Гобела Володимир Володимирович
кандидат економічних наук, доцент,
Львівський державний університет внутрішніх справ
ORCID: https://orcid.org/0000-0001-7438-2329

Лесик Назарій Андрійович
аспірант,
Львівський державний університет внутрішніх справ
ORCID: https://orcid.org/0000-0001-8116-5373

Leskiv Halyna, Hobela Volodymyr, Lesyk Nazarii
Lviv State University of Internal Affairs

Дослідження спрямоване на характеристику основних проблем забезпечення інформаційної безпеки в умовах впливу цифрових технологій. Доведено важливість аналізу основних проблем забезпечення інформаційної безпеки в сучасних умовах діджиталізації соціально-економічних систем та воєнних реалій сьогодення. Стаття спрямована на дослідження основних проблем забезпечення інформаційної безпеки в умовах впливу цифрових технологій, їх характеристики та дослідженні інших видів загроз, що сформувалися на даному етапі. Сукупність загально-теоретичних методів дослідження слугували методологією реалізації дослідження. В результаті, було визначено ключові проблеми забезпечення інформаційної безпеки в умовах впливу цифрових технологій, війни та воєнних загроз для інформаційної безпеки. Ідентифіковано основні проблеми у сфері забезпечення інформаційної безпеки організацій та підприємств. Виокремлено причини, що сприяли їх появі. Розроблено теоретичну модель протидії загрозам інформаційній безпеці підприємства. Розроблено низку рекомендацій для вирішення основних проблем забезпечення інформаційної безпеки підприємства. Запропоновано та обґрунтовано доцільність формування моделі реагування на проблеми забезпечення інформаційної безпеки для окремо взятої соціально-економічної системи.

Ключові слова: інформаційна безпека, модель, цифрові технології, забезпечення безпеки, безпека.

The study was aimed at characterizing the main problems of ensuring information security under the influence of digital technologies. The paper proved the importance of analyzing the main problems of ensuring information security of socio-economic systems in the conditions of digitization and military realities of nowadays. The article was aimed at researching the main problems of ensuring information security under the influence of digital technologies, and their characteristics and researching other types of threats that have formed at this stage. A set of general theoretical research methods served as the research implementation methodology. It is about the use of methods of theoretical analysis and synthesis, deduction, theoretical generalization and the modeling method. As a result, the key problems of ensuring information security under the influence of digital technologies, and war and military threats to information security were identified. An analysis of the provision of information security by representatives of Ukrainian business, in particular the financial sphere, at the beginning and during military operations on the territory of the state was carried out. The main problems in the field of ensuring information security of organizations and enterprises have been identified. The reasons contributing to their appearance are singled

out. A theoretical model for countering threats to the information security of the enterprise has been developed. The algorithm for building the model consisted in: determining the main elements of the model for countering threats to information security at the enterprise and their characteristics; the development of pre-modeling stages, which made it possible to form a preparatory basis for the model itself and to answer the question of relevance and the need to counter threats to the provision of information security at the enterprise; formation of the very model of ensuring information security at the enterprise. Some recommendations have been developed to solve the main problems of ensuring the information security of the enterprise. The expediency of forming a response model to the problems of ensuring information security for a separate socio-economic system was proposed and substantiated.

Keywords: information security, model, digital technologies, security assurance, security.

Постановка проблеми. Інформаційна безпека для будь-якої соціально-економічної системи – це вкрай важливий елемент, високий рівень якого залежить від багатьох факторів, як зовнішніх, так і внутрішніх. Можливо, саме інформаційна безпека є найбільш не постійною з усіх складових економічної безпеки. І це проявляється за рахунок постійної зміни технологій і різкого розвитку Індустрії 4.0, яка вже тут з нами і демонструє перші результати своєї появи. В таких умовах, не можливо просто постійно приймати одні і ті самі рішення для її забезпечення. Вона потребує нових рішень та заходів з врахуванням стану цифровізації як такої. З її забезпеченням завжди виникає ряд проблем, які не завжди виходить вирішувати. Останні зміни в Україні, призвели до суттєвого посилення питання забезпечення інформаційної безпеки але з початком військових дій, цього не достатньо. Не кращою ситуація є і з питанням забезпечення інформаційної безпеки на рівні окремо взятого підприємства.

Тому питання забезпечення інформаційної безпеки залишається вкрай актуальним завданням сьогодення.

Аналіз останніх досліджень і публікацій. Важливі аспекти проблем забезпечення інформаційної безпеки, розкривалися в роботах А. В. Войчика, С. В. Мельниченка, Т. О. Примака, Л. Ф. Романенка, Н. Д. Свірідової, Т. І. Ткаченка, Л. М. Шульгіної та інших. Теоретичною основою дослідження стали праці: Д. Мачека, І. Магдаленича, Н. Б. Редепа, С. Фенца, А. Екельхарта, Л. Пана, А. Томлінсона, З. Ф. Ерен-Догу, Х. Чанга, Х. Занга, А. Роя, А. Гупти, С. Дешмуха.

Однак настання пандемії і військових дій на території України, суттєво змінили ключові аспекти системи забезпечення інформаційної безпеки, що і зумовило вибір даної тематики та обумовило її актуальність.

Метою дослідження є характеристика основних проблем забезпечення інформаційної безпеки в умовах впливу цифрових технологій. Сукупність теоретичних методів дослідження слугували методологію під час проведеного аналізу.

Виклад основного матеріалу. В умовах військового стану та введення військових дій на багатьох регіонах країни, важко уявити, як можливо не то що збільшити але хоча би утримати бажаний рівень економічної безпеки та її складових. Проблем системи забезпечення інформаційної безпеки підприємства в України вистачає. Сюди можна віднести і постійні хакерські атаки ворога, і не спроможність в повному обсязі здійснити цифровізацію. Тут ми маємо і проблеми з постачання сучасних технологій для введення бізнесу в умовах Індустрії 4.0 і т.д.

Яскравим прикладом застосування заходів забезпечення інформаційної безпеки стали дії ПАТ КБ «Приватбанк», як миттєво переводив усю свою інформаційну базу на хмарні технології з метою не допущення їх втрати або викрадення ворогом. Сьогодні можна впевнено сказати, що проблем забезпечення інформаційної безпеки на будь-якому рівні, вистачає. Навіть якщо це стосується інформаційної безпеки особи. У сучасному світі спостерігаємо надто тісну взаємодію людини і цифрових технологій. Зворотного шляху немає і тому, і проблем буде лише більше.

Отже, для дослідження способів протидії загрозам для інформаційної безпеки підприємства слід розробити теоретичну модель. Першим кроком буде визначення основних елементів моделі протидії проблемам забезпечення інформаційної безпеки на підприємстві (табл. 1).

Окрім базових елементів, слід виділити і етапи премоделювання, які дозволяють сформувати підготовче підґрунтя для самої моделі. Такі етапи дозволяють відповісти на питання актуальності і чи взагалі є потреба в протидії проблемам забезпечення інформаційної безпеки на підприємстві (рис. 1).

Таблиця 1

Основні елементи моделі протидії проблемам забезпечення інформаційної безпеки на підприємстві

Елементи	Характеристика
Мета процесу моделювання і формування самої моделі	Формування моделі протидії проблемам забезпечення інформаційної безпеки на підприємстві
Ключова (цільова) аудиторія моделі	Відділ інформаційного забезпечення, служба безпеки та керівництво підприємства
Початкові дані та ресурси для досягнення мети	Фінансові, інформаційні та трудові ресурси підприємства
Програмне забезпечення моделювання	Організаційно-технічні засоби моделювання

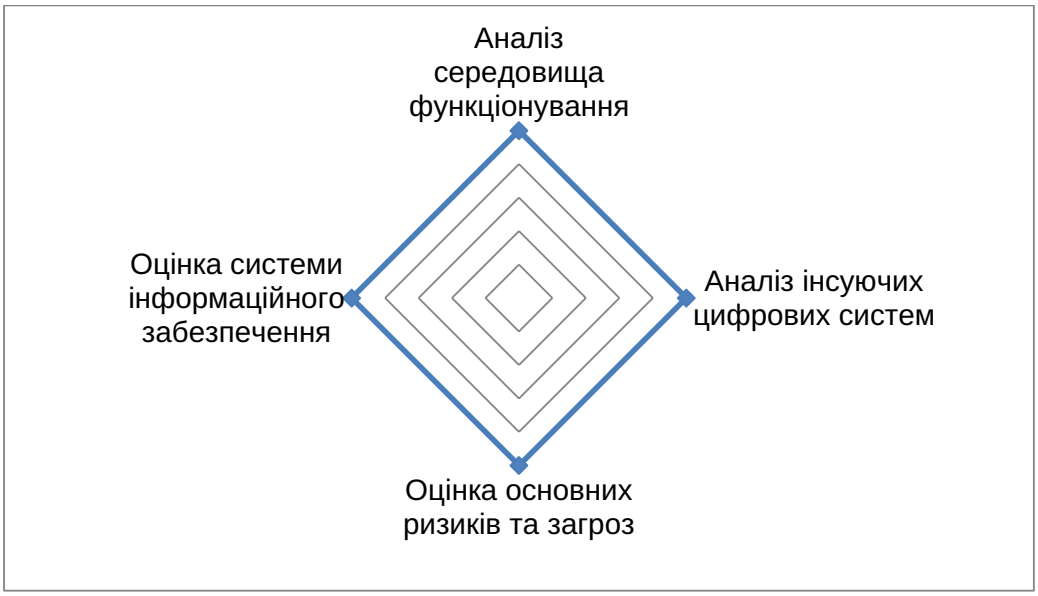

Рис. 1. Етапи моделювання протидії проблемам забезпечення інформаційної безпеки на підприємстві

Джерело: розроблено авторами

Останнім етапом нашого дослідження буде формування самої моделі протидії проблемам забезпечення інформаційної безпеки на підприємстві. Акцент при побудові моделі був зміщений на те, що потрібно для протидії загрозам, які засоби контролю та механізми слід застосувати і які результати повинні отримати в кінці. Розроблена модель носить теоретичний характер і виступає як інформаційна демонстрація механізму протидії проблемам забезпечення інформаційної безпеки на підприємстві (рис. 2).

Підсумовуючи, слід зазначити, що важливу роль у протидії проблемам забезпечення інформаційної безпеки на підприємстві в умовах впливу сучасних цифрових технологій відіграють не лише технічні засоби і технічне оснащення самої соціально-економічної системи та її структури, але і так звана «цифрова грамотність» працівників. Знання і розуміння нових технологій повинно виходити не лише з відповідного відділу інформаційної безпеки, але і від кожного працівника підприємства.

Висновки. Слід наголосити, що сьогодні, на території України ведуться військові дії, які суттєво загрожують усім складовим економічної та національної безпеки. Складно в таких умовах, говорити про шляхи забезпечення інформаційної безпеки окремо взятого підприємства, установи або ж соціально-економічної системи. Навіть до початку війни на території України, існували суттєві проблеми забезпечення безпеки на усіх рівнях. Прихід цифрових технологій та масова діджиталізація в системах, призвела до появи багатьох

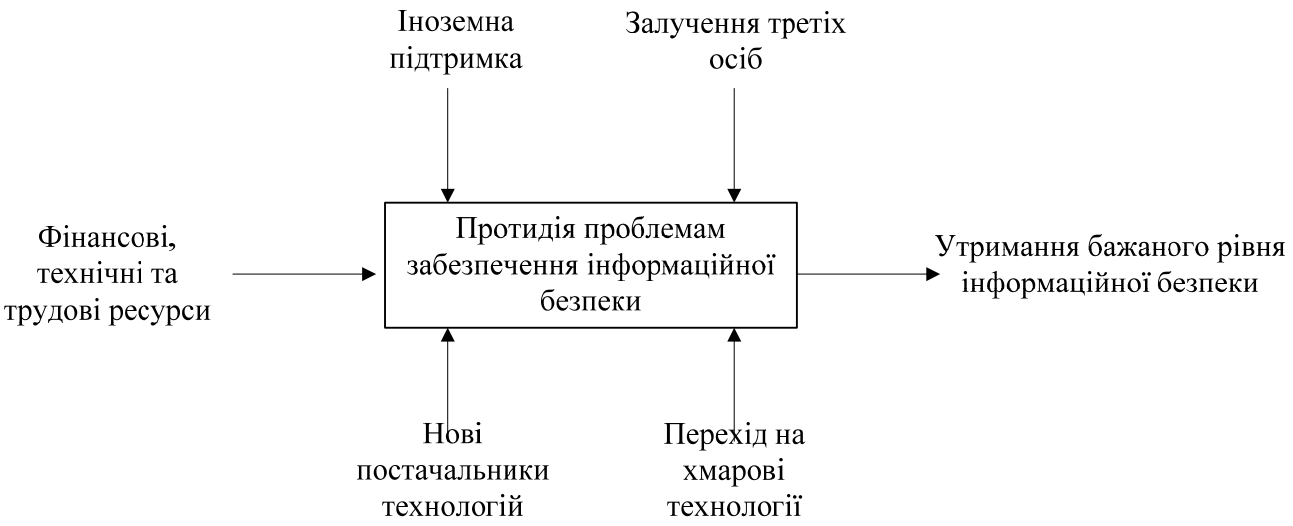

Рис. 2. Модель протидії проблемам забезпечення інформаційної безпеки на підприємстві

Джерело: розроблено авторами

проблем, які в Україні намагалися вирішувати. Але, з настанням військових дій, це поки, відклалося.

Результатом дослідження є сформована теоретична модель забезпечення інформаційної безпеки, проте її застосування має ряд обмежень. Перш за все, це стосується відсутності практичного застосування та не можливості використання методів прогнозування через присутність фактору невизначеності у стабілізаційній ситуації в Україні. Подальші дослідження повинні стосуватися питання зміцнення системи інформаційної безпеки вже у поствоєному стані.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Maček, D., Magdalenić, I., Ređep, N.B. A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. *International Journal of Safety and Security Engineering*. 2020. Vol. 10, no. 2, pp. 161–174. DOI: https://doi.org/10.18280/ijsse.100202.

2. Fenz, S., Ekelhart, A. Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy*. 2011. № 9 (2). P. 58–65. DOI: https://doi.org/10.1109/MSP.2010.117.

3. Pan, L., Tomlinson, A. A systematic review of information security risk assessment. *International Journal of Safety and Security Engineering*. 2016. № 6(2). P. 270–281. DOI: https://doi.org/10.2495/SAFE-V6-N2-270-281.

4. Eren-Dogu, Z. F. & Celikoglu, C. C., Information security risk assessment: Bayesian prioritization for group decision making. *International Journal of Innovative Computing, Information and Control*. 2012. № 8. P. 8001–8018.

5. Wei, G., Xhang, X., Zhang, X. & Huang, Z., Research on e-government information security risk assessment-based on fuzzy ahp and artificial neural network model. *Networking and Distributed Computing (IC-NDC)*, First International Conference on, IEEE. 2010. P. 218–221. DOI: http://dx.doi.org/10.1109/icndc.2010.52.

6. Roy, A., Gupta, A. & Deshmukh, S., Information security risk assessment in SCM. *Industrial Engineering and Engineering Management (IEEM)*. International Conference on, IEEE. 2013. P. 1002–1006. DOI: http://dx.doi.org/10.1109/ieem.2013.6962561.

REFERENCES:

1. Maček, D., Magdalenić, I., Ređep, N.B. (2020). A systematic literature review on the application of multicriteria decision making methods for information security risk assessment. *International Journal of Safety and Security Engineering*. Vol. 10, no. 2, pp. 161–174. DOI: https://doi.org/10.18280/ijsse.100202.

2. Fenz, S., Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. *IEEE Security & Privacy*, no 9 (2), pp. 58–65. DOI: https://doi.org/10.1109/MSP.2010.117.

3. Pan, L., Tomlinson, A. (2016). A systematic review of information security risk assessment. *International Journal of Safety and Security Engineering*, no 6(2), pp. 270–281. DOI: https://doi.org/10.2495/SAFE-V6-N2-270-281.

4. Eren-Dogu, Z. F. & Celikoglu, C. C. (2012). Information security risk assessment: Bayesian prioritization for group decision making. *International Journal of Innovative Computing, Information and Control*, no 8, pp. 8001–8018.

5. Wei, G., Xhang, X., Zhang, X. & Huang, Z. (2010). Research on e-government information security risk assessment-based on fuzzy and artificial neural network model. *Networking and Distributed Computing (IC-NDC).* First International Conference on, IEEE, pp. 218–221. DOI: http://dx.doi.org/10.1109/icndc.2010.52.

6. Roy, A., Gupta, A. & Deshmukh, S., (2013). Information security risk assessment in SCM. *Industrial Engineering and Engineering Management (IEEM)*. International Conference on, IEEE. pp. 1002–1006. DOI: http://dx.doi.org/10.1109/ieem.2013.6962561.