УДК 65.012
DOI: https://doi.org/10.32782/2311-844X/2024-1-13

Вінічук Марія Володимирівна
кандидат економічних наук, доцент,
доцент кафедри соціально-поведінкових,
гуманітарних наук та економічної безпеки,
Інститут управління, психології та безпеки
Львівського державного університету внутрішніх справ
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: https://orcid.org/0000-0002-6588-1254

Коваль Павло Євгенович
аспірант кафедри соціально-поведінкових,
гуманітарних наук та економічної безпеки,
Інститут управління, психології та безпеки
Львівського державного університету внутрішніх справ,
вулиця Городоцька, 26, Львів, 79000, Україна
ORCID: https://orcid.org/0009-0009-5581-0047

ПРОБЛЕМИ ЗАПОБІГАННЯ ТА ПРОТИДІЇ ЗАГРОЗАМ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ІТ-КОМПАНІЙ

Анотація. *Сучасні умови функціонування України як незалежної європейської держави, що перебуває у стані війни, характеризуються значним рівнем нестабільності та невизначеності, внаслідок чого загострюються проблеми безпеки інформаційного простору як на рівні держави, так і на рівні підприємств. У статті здійснено теоретичне обґрунтування проблемних аспектів забезпечення інформаційної безпеки ІТ-компаній та формування ними основних заходів щодо запобігання та протидії реальним і потенційним загрозам. Визначено сутність інформаційної безпеки ІТ-компаній, під якою пропонується розуміти стан захищеності інтересів ІТ-компаній від негативного впливу на інформаційні ресурси дестабілізуючих чинників зовнішнього і внутрішнього середовища. Виявлено основні проблеми забезпечення інформаційної безпеки ІТ-компаній, зокрема: посилення інформаційного впливу російської федерації; зростання чисельності та системності хакерських атак зі сторони країни-агресора; неспроможність суб'єктів господарювання в повній мірі здійснити процеси цифровізації; проблеми постачання сучасних технологій, необхідних для ведення бізнесу. Окреслено стратегічні пріоритети формування системи заходів запобігання та протидії загрозам інформаційній безпеці ІТ-компаній, що передбачають розроблення моделі запобігання та протидії загрозам інформаційній безпеці ІТ-компаній, основними елементами якої є мета, цільова аудиторія, ресурсне забезпечення та програмне забезпечення. Доведено що забезпечення інформаційної безпеки ІТ-компаній здійснюється в межах реалізації Стратегії інформаційної безпеки України. З метою попередження негативного впливу загроз зовнішнього і внутрішнього середовища на рівень інформаційної безпеки ІТ-компаній, обґрунтовано пропозицію формування ефективної системи управління інформаційними ресурсами та забезпечення надійного захисту каналів передавання інформації.*

Ключові слова: *інформаційна безпека, ІТ-компанії, загрози, інформаційні технології, цифровізація, інформаційне середовище.*

Vinichuk Maria, Koval Pavlo
Lviv State University of Internal Affairs

PROBLEMS OF PREVENTION AND COUNTERING THE INFORMATION SECURITY THREATS OF IT COMPANIES

Abstract. *The current conditions of the functioning of Ukraine as an independent European state in a state of war are characterized by a significant level of instability and uncertainty, as a result of which the problems of the security of the information space are becoming more acute both at the level of the state and at the level of*

enterprises. The article provides a theoretical substantiation of the problematic aspects of ensuring IT companies' information security and their formation of basic measures to prevent and counter actual and potential threats. The essence of information security of IT companies is determined, under which it is proposed to understand the state of protection of the interests of IT companies from the negative impact on information resources of destabilizing factors of the external and internal environment. The main problems of ensuring information security of IT companies were identified, in particular: strengthening of the informational influence of the Russian Federation; an increase in the number and systematicity of hacker attacks by the aggressor country; failure of business entities to fully implement digitization processes; problems of supplying modern technologies necessary for conducting business. The strategic priorities of forming a system of measures to prevent and counter threats to information security of IT companies are outlined, which involve the development of a model for preventing and countering threats to information security of IT companies, the main elements of which are the goal, target audience, resource provision and software. It has been proven that the provision of information security of IT companies is carried out within the framework of the implementation of the Information Security Strategy of Ukraine. In order to prevent the negative impact of threats from the external and internal environment on the level of information security of IT companies, the proposal to form an effective system for managing information resources and ensuring reliable protection of information transmission channels is substantiated.

Key words: *information security, IT companies, threats, information technologies, digitalization, information environment.*

Вступ. На сучасному етапі розвитку світових господарських відносин актуалізуються процеси цифровізації економіки та суспільства, внаслідок чого виникають вагомі проблеми інтенсифікації розвитку інформаційних технологій та глобальних мереж, які широко використовують інтерактивні засоби поширення інформації та швидкого й миттєвого отримання необхідних відомостей. Зазначені умови свідчать про формування глобального інформаційного суспільства, чільне місце у якому належить ІТ-компаніям як суб'єктам опрацювання інформації в системі забезпечення формування й реалізації інформаційної політики на різних рівнях суспільних відносин. Однак, досягнути високих показників ефективності діяльності ІТ-компаній в сучасних умовах нестабільності та невизначеності надзвичайно важко, що обумовлено дестабілізуючим впливом на них чинників зовнішнього та внутрішнього середовища. Тому, актуалізується необхідність забезпечення достатнього рівня інформаційної безпеки ІТ-компаній та їх захисту від негативного впливу таких факторів як політична обстановка у світі, рівня розвитку інформаційно-телекомунікаційних технологій та внутрішньополітичного становища, адже, події сьогодення засвідчують, що інформаційний вплив є вагомим інструментом переформатування світосприйняття у свідомості населення та дестабілізуючим чинником діяльності суб'єктів господарювання. Стає очевидним, що проблематика дослідження інформаційної безпеки ІТ-компаній переміщується на передній план та потребує детального вивчення основних загроз, які провокують зниження її рівня.

Матеріали та методи. Дослідження проблем запобігання та протидії загрозам інформаційній безпеці ІТ-компаній актуалізуються в сучасних умовах функціонування держави, суспільства та суб'єктів господарювання. Вагомий внесок у пошук шляхів їх вирішення зробили такі науковці як В. Гобела, У. Ільницька, М. Копитко, Г. Леськів, В. Новицький, Т. Слінько, О. Федченко та багато інших. Однак, незважаючи на їх вагомий науковий доробок проблеми забезпечення інформаційної безпеки досі залишаються невирішеними та потребують поглибленого вивчення.

Метою статті є дослідження основних аспектів та проблемних питань запобігання та протидії загрозам інформаційній безпеці ІТ-компаній.

Для реалізації дослідження використано низку загальнонаукових методів, а саме: системний аналіз та синтез для визначення сутності інформаційної безпеки та її загроз, порівняння з метою виявлення проблем забезпечення інформаційної безпеки ІТ-компаній, узагальнення та систематизації для формування основних заходів щодо запобігання та протидії загрозам інформаційній безпеці ІТ-компаній.

ISSN 2311-844X

Результати. Діяльність ІТ-компаній в сучасних умовах характеризується високим ступенем нестабільності та невизначеності, адже поява значних небезпечних чинників дестабілізуючого впливу спричинює виникнення вагомих загроз в інформаційній сфері, які провокують зниження рівня інформаційної безпеки та появу нових видів ризиків операціям, які здійснюються у віртуальному просторі. Очевидно, що в період повномасштабного вторгнення російської федерації на територію України загострилася необхідність посилення безпеки інформаційного простору не лише ІТ-компаній, а й інформаційного суверенітету країни, адже, інформаційні технології дедалі частіше використовуються з метою здійснення негативних інформаційно-психологічних впливів. Тому, науково-практичні розробки у сфері інформаційної безпеки ІТ-компаній та виявлення проблемних аспектів забезпечення процесів запобігання та протидії її загрозам є вкрай важливими та необхідними.

Варто зазначити, що в даному контексті ведеться активна наукова дискусія. Зокрема, низка вітчизняних та зарубіжних вчених ґрунтовно вивчають окреслену проблематику та працюють над забезпеченням ефективних механізмів запобігання та протидії загрозам інформаційній безпеці як на макрорівні, так і на мікрорівні. У. Ільницька [1, с. 28–29] інформаційну безпеку вважає інтегрованою складовою інших видів безпеки та стверджує, що вона відображає стан захищеності життєво важливих інтересів підприємства, суспільства і держави від негативного впливу неповної й недостовірної інформації, несанкціонованого її поширення, а також попереджує негативні наслідки функціонування інформаційних технологій. При цьому, науковиця акцентує увагу на небезпеці виникнення загроз інформаційній безпеці, під якими розуміє сукупність умов та чинників, які провокують небезпеки через можливість негативного інформаційного впливу на свідомість й поведінку суб'єктів, на інформаційні ресурси та на інформаційно-технічну інфраструктуру.

Г. Леськів, В. Гобела та Н. Лесик [2] поглибили дослідження інформаційної безпеки підприємств в умовах війни росії проти України та виявили низку проблем її забезпечення, до найбільш вагомих із яких віднесли: (1) зростання чисельності та системність хакерських атак зі сторони країни-агресора; (2) неспроможність суб'єктів господарювання в повній мірі здійснити процеси цифровізації; (3) проблеми постачання сучасних технологій, необхідних для ведення бізнесу. Водночас, науковці пропонують формування моделі протидії проблемам забезпечення інформаційної безпеки підприємства, основними елементами якої вважають засоби й механізми контролю за інформаційними потоками.

На відміну від зазначених вчених, О. Федченко [3, с. 129] пропонує інформаційну безпеку ІТ-компаній розглядати як складову інформаційної безпеки держави, а її сутність визначає як складне системне й багаторівневе явище, забезпечення оптимального рівня якої істотно залежить від інформаційної стратегії держави. Крім того, О. Федченко [3, с. 130] визначає основні загрози інформаційній безпеці підприємств, в т.ч. ІТ-компаній, зокрема, стверджує, що в сучасних умовах найбільш вагомий загрозливий вплив мають глобальні виклики, інформаційна політика російської федерації, функціонування соціальних мереж, низький рівень медіа-грамотності на фоні стрімкого розвитку цифрових технологій та інформаційні маніпуляції.

Цікавим є підхід В. Новицького [4, с. 114] до визначення проблем забезпечення інформаційної безпеки підприємств і ІТ-компаній, який передбачає формування системи протидії загрозам інформаційній безпеці з точки зору їх розподілу на загрози, що зумовлені технологіями інформаційно-комунікаційних процесів та ті, що обумовлені соціальними чинниками. При цьому, науковець акцентує увагу на доцільності та важливості прийнятої Стратегії інформаційної безпеки [5], яка сформувала фундамент для визначення основних завдань щодо недопущення кризових явищ у вітчизняному інформаційному просторі та щодо визначення основних заходів, спрямованих на посилення інформаційної безпеки на рівні підприємств.

Водночас, Т. Слінько [6, с. 83] виокремила не лише основні загрози інформаційній безпеці, а й запропонувала шляхи їх подолання та стверджує, що вирішення проблем запобігання та протидії загрозам інформаційній безпеці залежать від своєчасності й ефективності організаційно-правових та організаційно-технічних механізмів забезпечення захисту інформаційного простору в країні, внаслідок чого суб'єкти господарювання одержать можливість протистояти викликам і небезпекам сучасності. На думку вченої, істотно посилити інформаційну безпеку як на макрорівні, так і на мікрорівні можна за допомогою формування ефективної системи управління інформаційними ресурсами та шляхом забезпечення надійного захисту каналів передавання інформації.

Досліджуючи особливості функціонування підприємств в умовах глобального інноваційного розвитку та цифровізації, М. Копитко та М. Вінічук [7] дійшли висновку, що забезпечення інформаційної безпеки підприємств і ІТ-компаній є одним із вагомих елементів забезпечення їх конкурентоспроможності та запорукою успішного розвитку й досягнення позитивних фінансових результатів.

Стає очевидним, що в умовах сучасності існує значна кількість вагомих проблем забезпечення інформаційної безпеки в Україні та критично вони постають по відношенню до суб'єктів господарювання, зокрема, до ІТ-компаній. Наявність небезпечних загроз інформаційній безпеці є доведеною, а їх запобігання та протидія потребує виважених кроків як зі сторони керівництва компаній, так зі сторони держави.

Вирішити проблеми забезпечення інформаційної безпеки ІТ-компаній, які часто піддаються хакерським атакам зі сторони країни-агресора, одномоментно неможливо, попри вагомі напрацювання в даному напрямку та наявність механізмів протидії загрозам. Вагоме значення в даному контексті має розроблення власної моделі протидії проблемам забезпечення інформаційної безпеки ІТ-компаній та запобіганню наявним і потенційним загрозам, яка повинна включати декілька елементів, зокрема: (1) мету формування моделі; (2) цільову аудиторію; (3) ресурсне забезпечення; (4) програмне забезпечення, характеристику яких вважаємо з доцільне відобразити на рис. 1.

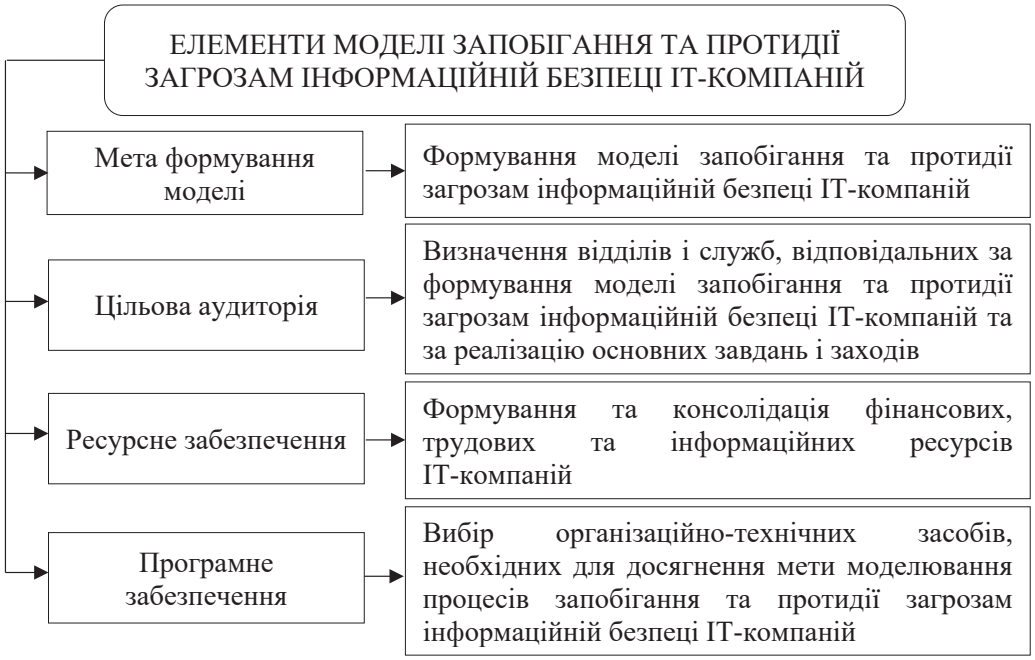

Рис. 1. Основні елементи моделі запобігання та протидії загрозам інформаційній безпеці ІТ-компаній

Джерело: сформовано авторами

Реалізація моделі запобігання та протидії загрозам інформаційній безпеці ІТ-компаній повинна відбуватися на декількох етапах, які включають необхідність проведення аналізу середовища функціонування ІТ-компаній та існуючих сучасних цифрових систем, оцінку системи інформаційного забезпечення кожної ІТ-компанії та її спроможності протистояти викликам і небезпекам, а також оцінку основних ризиків і загроз.

Висновки. Таким чином, результати проведеного дослідження показали, що в умовах сьогодення існують вагомі проблемні питання запобігання та протидії загрозам інформаційній безпеці ІТ-компаній. На підставі аналізу існуючого наукового доробку можна стверджувати, що забезпечення інформаційної безпеки ІТ-компаній здійснюється в межах реалізації Стратегії інформаційної безпеки України, а для формування ефективних заходів запобігання та протидії загрозам інформаційній безпеці ІТ-компаній необхідно розробляти спеціальні моделі, основними елементами яких виступають: мета, цільова аудиторія, ресурсне забезпечення та програмне забезпечення. Встановлено, що інформаційна безпека ІТ-компаній – це стан захищеності їх інтересів від негативного впливу на інформаційні ресурси дестабілізуючих чинників зовнішнього і внутрішнього середовища. Виявлено основні проблеми запобігання та протидії загрозам інформаційній безпеці ІТ-компаній, серед найбільш вагомих із яких є посилення інформаційного впливу російської федерації; зростання чисельності та системності хакерських атак зі сторони країни-агресора; неспроможність суб'єктів господарювання в повній мірі здійснити процеси цифровізації; проблеми постачання сучасних технологій, необхідних для ведення бізнесу. З метою посилення інформаційної безпеки ІТ-компаній доцільним виявляється формування ефективної системи управління інформаційними ресурсами та забезпечення надійного захисту каналів передавання інформації.

Список використаних джерел:

1. Ільницька У. Інформаційна безпека України: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. *Гуманітарні візії*. 2016. Вип. 2. № 1. С. 27–32. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf

2. Леськів Г.З., Гобела В.В., Лесик Н.А. Характеристика основних проблем забезпечення інформаційної безпеки в умовах впливу цифрових технологій. *Економіка та суспільство*. 2022. Вип. 43. DOI: https://doi.org/10.32782/2524-0072/2022-43-8

3. Федченко О. Аналіз факторів та сучасних загроз інформаційній безпеці держави у контексті забезпечення національної безпеки України. *Journal of Scientific Papers «Social Development and Security»*. 2022. Vol. 12. № 3. С. 128–134. DOI: https://doi.org/10.33445/sds.2022.12.3.11

4. Новицький В.Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право.* 2022. № 1(40). С. 111–118. DOI: https://doi.org/10.37750/2616-6798.2022.1(40).254349

5. Про Стратегію інформаційної безпеки : рішення Ради національної безпеки і оборони України від 15.10.2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text

6. Слінько Т.С. Сучасні загрози інформаційній безпеці країни й шляхи їх подолання. *Український часопис конституційного права.* 2021. № 4. С. 77–84. URL: https://www.constjournal.com/wp-content/uploads/issues/2021-4/pdfs/6-tetiana-slinko-suchasni-zahrozy-informatsiyniy-bezpetsi-krainy-shliakhy-ikh-podolannia.pdf

7. Копитко М.І., Вінічук М.В. Конкурентоспроможність підприємств в умовах глобального інноваційного розвитку економіки. *Вчені записки Університету «КРОК»*. 2022. № 3(67). С. 62–68. DOI: https://doi.org/10.31732/2663-2209-2022-67-62-68

References:

1. Ilnytska U. (2016) Informatsiyna bezpeka Ukrayiny: suchasni vyklyky, zahrozy ta mekhanizmy protydiyi nehatyvnym informatsiyno-psykholohichnym vplyvam [Information Security of Ukraine: modern challenges, threats and countermeasures against negative informational and psychological influences]. *Humanita-*

rian visions, vol. 2, no. 1, pp. 27–32. Available at: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/4352/ilnicka0.pdf (in Ukrainian)

2. Leskiv G.Z., Gobela V.V., Lesyk N.A. (2022) Kharakterystyka osnovnykh problem zabezpechennya informatsiynoyi bezpeky v umovakh vplyvu tsyfrovykh tekhnolohiy [Characterization of the main problems of ensuring information security under the influence of digital technologies]. *Economy and Society,* vol. 43. DOI: https://doi.org/10.32782/2524-0072/2022-43-8 (in Ukrainian)

3. Fedchenko O. (2022) Analiz faktoriv ta suchasnykh zahroz informatsiyniy bezpetsi derzhavy u konteksti zabezpechennya natsional′noyi bezpeky Ukrayiny [Analysis of factors and modern threats to the information security of the state in the context of ensuring the national security of Ukraine]. *Journal of Scientific Papers "Social Development and Security",* vol. 12, no. 3, pp. 128–134. DOI: https://doi.org/10.33445/sds.2022.12.3.11 (in Ukrainian)

4. Novytsky V.Ya. (2022) Stratehichni zasady zabezpechennya informatsiynoyi bezpeky v suchasnykh umovakh [Strategic principles of ensuring information security in modern conditions]. *Information and Law*, no. 1(40), pp. 111–118. DOI: https://doi.org/10.37750/2616-6798.2022.1(40).254349 (in Ukrainian)

5. Pro Stratehiyu informatsiynoyi bezpeky: rishennya Rady natsional′noyi bezpeky i oborony Ukrayiny vid 15.10.2021 r. № 685/2021 [About the Information Security Strategy: Decision of the National Security and Defense Council of Ukraine No. 685/2021 of October 15, 2021]. Available at: https://zakon.rada.gov.ua/laws/show/n0080525-21#Text (in Ukrainian)

6. Slinko T.S. (2021) Suchasni zahrozy informatsiyniy bezpetsi krayiny y shlyakhy yikh podolannya [Modern threats to the country's information security and ways to overcome them]. *Ukrainian Journal of Constitutional Law,* no. 4, pp. 77–84. Available at: https://www.constjournal.com/wp-content/uploads/issues/2021-4/pdfs/6-tetiana-slinko-suchasni-zahrozy-informatsiyniy-bezpetsi-krainy-shliakhy-ikh-podolannia.pdf (in Ukrainian)

7. Kopytko M.I., Vinichuk M.V. (2022) Konkurentospromozhnist′ pidpryyemstv v umovakh hlobal′noho innovatsiynoho rozvytku ekonomiky [Competitiveness of enterprises in the conditions of global innovative development of the economy]. *Scientific notes of the "KROK" University*, no. 3(67), pp. 62–68. DOI: https://doi.org/10.31732/2663-2209-2022-67-62-68 (in Ukrainian)