DOI: https://doi.org/10.15407/etet2023.01.047
УДК: 338.242(477)
JEL: E60, E61, H19, O29

Володимир Міщенко

УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ В СИСТЕМІ ЗАБЕЗПЕЧЕННЯ НАЦІОНАЛЬНО УКОРІНЕНОЇ СТІЙКОСТІ ЕКОНОМІЧНОГО РОЗВИТКУ

У ході дослідження визначено, що збільшення обсягів і розширення сфер використання цифрових технологій об'єктивно обумовлюють виникнення кіберзагроз і наражають усіх учасників цифрових екосистем на кіберризики, що стримує економічний розвиток. Доведено, що наявність широкого кола чинників, які формують кібербезпеку та кіберстійкість, потребує реалізації комплексного підходу до формування захисних стратегій діяльності підприємств і установ. Визначено, що процес організації управління кіберстійкістю повинен ґрунтуватися на розробленні комплексних систем кіберзахисту, які засновані на чітких політиках, правилах і стратегіях раннього виявлення, попередження та мінімізації наслідків реалізації кіберзагроз з використанням широкого спектра технічних, технологічних, організаційних, управлінських і регуляторних за-

Міщенко Володимир Іванович (mishchenko.ie@ief.org.ua), д-р екон. наук, проф., завідувач сектору цифрової економіки відділу економічної теорії ДУ "Інститут економіки та прогнозування НАН України". ORCID ID: http://orcid.org/0000-0002-8565-2686

Стаття знайомить з результатами дослідження, виконаного в рамках наукового проєкту "Формування засад національно укоріненої стійкості та безпеки економічного розвитку України в умовах гібридної системи "мир-війна" (держреєстраційний №0123U100965).

Цитування: Міщенко В. І. Управління кібербезпекою в системі забезпечення національно укоріненої стійкості економічного розвитку. *Економічна теорія*. 2023. №1. С. 47–72. DOI: https://doi.org/10.15407/etet2023.01.047

ходів. Обґрунтовано необхідність розроблення загальнодержавної стратегії та програми дій органів влади у сферах законодавства, регулювання, нагляду та контролю за станом кібербезпеки. Доведено, що національна стратегія кіберзахисту повинна передбачати ефективні заходи щодо захисту об'єктів критичної інфраструктури, органів державної влади та населення, а також систему регуляторних і наглядових заходів.

Встановлено, що першочерговим завданням організації та функціонування систем кіберзахисту повинен бути захист цифрових активів і ресурсів підприємств та їхніх клієнтів. З метою посилення інституційної спроможності органів влади для ефективної підтримки національної екосистеми кібербезпеки розроблено структурно-логічну схему взаємодії підприємств і Державного центру кіберзахисту України в процесі обміну інформацією про кіберінциденти, а також наведено практичні рекомендації щодо взаємодії об'єктів критичної інфраструктури та органів державного регулювання, які можуть бути використані з метою забезпечення національно укоріненої стійкості та безпеки економічного розвитку України в умовах гібридної системи "мир-війна".

Ключові слова: цифрові технології, цифрові інструменти; цифрова інфраструктура; кібербезпека; кіберстійкість; система управління кіберстійкістю, кіберзагроза; кіберризик.

CYBER SECURITY MANAGEMENT IN THE SYSTEM FOR ENSURING NATIONALLY ROOTED RESILIENCE OF ECONOMIC DEVELOPMENT

Volodymyr Mishchenko *(mishchenko.ie@ief.org.ua)*, doctor of economic sciences, professor; Head of the Sector of Digital Economy of the "Institute of Economics and Forecasting of NAS of Ukraine". ORCID ID: http://orcid.org/0000-0002-8565-2686

In the course of the study, it has been found that the increase in volumes and the expansion of the spheres of the use of digital technologies objectively cause the emergence of cyber threats and expose all participants of digital ecosystems to cyber risks, which restrains economic development. It has been proven that the presence of a wide range of factors that shape cyber security and cyber resilience requires the implementation of a comprehensive approach to the formulation of protective strategies of companies and institutions. The article argues that the process of organizing cyber resilience management should be based on the development of comprehensive cyber protection systems based on clear policies, rules and strategies for early detection, preven-

tion and minimization of consequences of the implementation of cyber threats using a wide range of technical, technological, organizational, managerial and regulatory measures. The author justifies the need to develop national strategy and program for the authorities in the spheres of legislation, regulation, supervision and control over the state of cyber security. He proves that the national cyber defense strategy should provide for effective measures to protect critical infrastructure objects, state authorities and the population, as well as a system of regulatory and supervisory measures.

The author establishes that the primary task for the organization and operation of cyber protection systems should be the protection of digital assets and of the companies' resources and their customers. In order to strengthen the institutional capacity of authorities to effectively support the national cyber security ecosystem, a structural and logical scheme of interaction between companies and the State Cyber Protection Center of Ukraine in the process of exchanging information about cyber incidents has been developed, and practical recommendations have been provided for the interaction between critical infrastructure objects and state regulatory bodies, which can be used to ensure nationally rooted stability and security of Ukraine's economic development in a hybrid "peace-war" system.

Key words: digital technologies, digital tools; digital infrastructure; cyber security; cyber resilience; cyber resilience management system, cyber threat; cyber risk

Головні поняття та взаємозв'язки в системі забезпечення кіберстійкості

Упродовж останніх десятиліть відбувається постійне збільшення обсягів і розширення сфер використання цифрових технологій, поширення Інтернету речей, гібридних і віддалених форм роботи, розвиток соціальних мереж, підвищення рівня "цифрової залученості" населення тощо, що об'єктивно обумовлює виникнення кіберзагроз і наражає всіх учасників цифрових екосистем на кіберризики, які мають специфічні форми прояву та можуть негативно впливати на різноманітні сфери діяльності *(Бандура,* 2020, С. 83*; Гриценко,* 2022а, С. 34*; Липов,* 2022, С. 35; *Яненкова,* 2020, С. 89).

Специфіка використання ІК-технологій потребує уточнення сутності головних понять, які використовуються в системі управління цифровими ризиками, та характеристики їх взаємозв'язків у процесі забезпечення кіберстійкості. На наш погляд, кіберзагрозу

варто розглядати як певну фактичну або потенційну подію (інцидент, явище, чинник), яка може порушити стабільне функціонування обладнання, програмного забезпечення або ІК-систем і спричинити збитки, втрату ресурсів чи активів або до інші небажані результати.

Поняття кіберризику характеризує ймовірність виникнення втрат, неодержання доходів або додаткових витрат унаслідок реалізації кіберзагроз. На практиці кіберризики, зазвичай, відносять до операційних ризиків *(Вишневський,* 2022, С. 54; *Філіпенко,* 2022, С. 49; *Mishchenko et al.,* 2022, P. 149), а головними причинами їх виникнення можуть бути недостатній рівень захисту ІК-систем і каналів зв'язку; несвоєчасне оновлення програмного забезпечення і технічних засобів; порушення мережевого протоколу віддаленого робочого місця; зараження програмного забезпечення; шкідливі програми та програми-вимагачі; несанкціоновані дії співробітників, шахрайство або інші зловмисні дії. Тому завдання управління кіберризиками полягає у зниженні ймовірності їх виникнення та мінімізації розмірів потенційних втрат, а заходи щодо підвищення ефективності управління повинні бути спрямовані насамперед на поліпшення техніко-технологічних характеристик ІК-систем, обладнання, програмного забезпечення та вдосконалення управління підприємством загалом *(Міщенко, Науменкова,* 2022, С. 147; *Mishchenko et al.,* 2021, P. 196; *Mishchenko et al.,* 2019, P. 47).

Під кібербезпекою, на наш погляд, слід розуміти організовану на певному рівні управління систему захисту від кіберзагроз (систему кіберзахисту), яка є сукупністю взаємопов'язаних технічних, організаційних, правових та управлінських заходів, спрямованих на запобігання кіберінцидентам, і характеризує потенційну кіберстійкість об'єкта захисту до впливу кіберзагроз або як можливість убезпечення від негативних наслідків їх реалізації, тобто як можливість забезпечення кіберстійкості.

Через комплексний характер і різноманітність форм прояву найбільш складним для визначення є поняття "кіберстійкість", яке часто ототожнюють з поняттям "кібербезпека". Наприклад, Р. Росс

зі співавторами визначає кіберстійкість як здатність підприємства передбачати, протистояти, відновлюватися та адаптуватися до стресів і кібератак, які відбуваються з використанням цифрових технологій та цифрових інструментів. Тому підтримка належного рівня кіберстійкості покликана забезпечити досягнення підприємством своєї місії та бізнес-цілей, які залежать від рівня надійності функціонування та ефективності використання кіберресурсів *(Ross et al., 2021).*

Таким чином, взаємозв'язок між поняттями "кіберзагроза", "кібербезпека", "кіберризик" і "кіберстійкість" можна визначити такою формулою: *кіберризик виникає внаслідок реалізації кіберзагроз через низький рівень організації системи кібербезпеки, яка не підтримує належний рівень кіберстійкості* певного об'єкта, процесу або явища.

Особливість управління кіберризиками полягає у необхідності пошуку балансу між необхідним (і достатнім) рівнем кіберстійкості та частотою і масштабами виникнення кіберзагроз, який постійно порушується через стрімкий розвиток цифрових технологій. Крім того, практика забезпечення кіберстійкості показала, що традиційний підхід до управління ризиками на основі оцінки співвідношення "ризик-вигода" в механізмі забезпечення кіберстійкості використовувати дуже складно, оскільки він не відповідає природі кібербезпеки: навіть одна кібератака може припинити існування підприємства.

У зв'язку з цим виникає потреба у розробленні для кожного об'єкта кіберзахисту системи індикаторів, які б характеризували мінімально допустимий (базовий) рівень його кібербезпеки. Водночас варто зазначити, що окремі індикатори повинні бути універсальними (наприклад, використання програмного забезпечення з вбудованими кодами, єдині стандарти доступу до даних), а інші – індивідуальними, щоб врахувати специфіку діяльності та рівень "цифрового охоплення" кожного підприємства.

Зважаючи на тенденцію до розширення спектра потенційних кіберзагроз і необхідність постійної підтримки належного рівня кіберстійкості, виникає потреба в розробленні *комплексних систем*

кіберзахисту підприємств, організацій та установ, які повинні ґрунтуватися на чітких політиках, правилах і стратегіях раннього виявлення, попередження та мінімізації наслідків реалізації кіберзагроз з використанням широкого спектра технічних, технологічних, організаційних, управлінських і регуляторних заходів *(Міщенко, Науменкова,* 2019, С. 118; *Міщенко,* 2022, С. 72; *Скрипниченко,* 2022, С. 37). До того ж кібербезпека та кіберстійкість повинні стати пріоритетом подальших цифрових трансформацій як на рівні підприємства, так і на рівні окремих галузей та країни загалом, забезпечуючи цифровий суверенітет, безпеку держави та національно укорінений економічний розвиток.

На відміну від традиційного підходу до управління фінансовими та нефінансовими ризиками, захисні цифрові стратегії повинні ґрунтуватися на дотриманні технічних і технологічних стандартів для інформаційних систем, обладнання, мереж і даних, а першочерговим завданням організації та функціонування систем кіберзахисту повинен бути *захист цифрових активів і ресурсів підприємств та їхніх клієнтів*. Посилення кіберзагроз і необхідність вдосконалення управління кіберризиками потребують розроблення нових методів їх попередження, виявлення та реагування.

Отже, **мета статті** – охарактеризувати методологічні та методичні засади забезпечення кіберстійкості національної економіки та обґрунтувати першочергові заходи щодо ефективного функціонування систем кіберзахисту з метою підтримки національно укоріненої стійкості економічного розвитку України.

Стан і передумови виникнення кіберзагроз і кіберризиків

Через значні обсяги інформаційних потоків і високий ступінь залученості до цифрового простору сьогодні практично вже не існує ні підприємств, ні фізичних осіб, які б тою чи іншою мірою не стикалися з кіберзагрозами та не наражалися на цифрові ризики, а більшість із них вже мають певний негативний досвід. За даними компанії McKinsey, в 2020 році кожна людина на планеті щосе-

кунди створювала 1,7 мегабайти даних, а близько 25% працівників у розвинених країнах 3–5 днів на тиждень працювали віддалено (*Boehm et al.,* 2022). У 2022 р. за одну хвилину в Інтернеті надсилалось майже 200 млн електронних листів, завантажувалося 500 годин контенту YouTube, публікувалося 695 тис. історій в Instagram, надсилалось 69 млн повідомлень WhatsApp, здійснювалося 9132 з'єднання в LinkedIn[1]. Така динаміка інформаційних потоків з використанням нових технологій та ІК-мереж неминуче призводить до того, що кількість і рівень кіберзагроз постійно зростають, а значить, збільшується й кількість потенційних кіберризиків.

Найчастіше зловмисники здійснюють кіберзлочини, використовуючи ІК-мережі з метою несанкціонованого доступу до даних або інших цифрових активів, під час оновлення програмного забезпечення, в разі доступу до персональної та корпоративної пошти, облікових записів співробітників підприємств та установ тощо. За даними ФБР США, у 2021 році в США було зареєстровано майже 850 тис. скарг на кіберзлочини, що на 55 тис. більше, ніж у 2020 році[2].

Найбільш поширеними видами кіберзагроз є фішинг, викрадення або пошкодження корпоративних і персональних даних, BEC/EAC-атаки, програми-вимагачі, зловмисна інсайдерська діяльність та інші. Наприклад, лише на початку пандемії COVID-19, у лютому–березні 2020 р., кількість атак програм-вимагачів збільшилась на 148%, а кількість фішингових атак за січень–лютий 2020 р. зросла на 510% (*Boehm et al.,* 2022). Разом з тим, як свідчить аналіз Звіту ФБР про злочини в Інтернеті, найбільших збитків підприємствам і громадянам завдають BEC/EAC-атаки, шахрайство, зокрема, на довірі, з інвестиціями та платежами, а також крадіжка особистих даних і спуфінг (табл. 1).

[1] Global Cybersecurity Outlook 2022. Insight Report. WEF. January 2022. URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (дата звернення: 15.02.2023)

[2] Facts + Statistics: Identity theft and cybercrime. Insurance Information Institute. 2022. URL: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (дата звернення: 22.02.2023)

Таблиця 1

Втрати від окремих видів кіберзлочинності в США в 2018–2020 роках, *млн дол.*

Вид кіберзлочину, (сфера шахрайства)	**2018**	**2019**	**2020**	**Збільшення (+), зменшення (-) у 2020 р. до 2018 р.,** *%*
Компрометація корпоративної пошти (BEC/EAC)	1297,8	1776,5	1866,6	43,8
Шахрайство на довірі	362,5	475,0	600,2	65,6
Шахрайство з інвестиціями	252,9	222,2	336,5	33,1
Шахрайство з платежами	183,8	196,6	265,0	44,2
Крадіжки особистих даних	100,4	160,3	219,5	118,6
Спуфінг	70,0	300,5	216,5	2,1 раза
Нерухомість/Оренда	149,5	221,4	213,2	42,6
Витік персональних даних	148,9	120,1	194,5	30,6
Технічна підтримка	38,7	54,0	146,5	2,8 раза
Витоки корпоративних даних	117,7	53,4	128,9	9,5
Шахрайство з кредитними картками	89,0	111,5	129,8	45,8
Шахрайство на основі уособлення з урядом	64,2	124,3	109,9	71,2
Вимагання	83,4	107,5	70,9	-15,0
Лотерейний бізнес, спадщина	60,2	48,6	61,1	1,5
Фішинг (вішинг, смішинг, фармінг)	48,2	57,8	54,2	12,4
Програми-вимагачі	3,6	9,0	29,2	7,1 раза
Сфера охорони здоров'я	4,4	1,1	29,0	5,6 раза

Джерело: складено на основі: Internet Crime Report. FBI. 2020. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (дата звернення: 10.03.2023)

За даними Інституту страхової інформації США, найчастіше викрадення персональних даних громадян відбувається через їхню необачність і довірливість при оформленні державних пільг (32,9%), у процесі використання кредитних карток (29,7%), а також при користуванні електронною поштою і соціальними мережами (22,9%) (табл. 2).

Таблиця 2

Головні види викрадення персональних даних громадян США в 2021 році

Види крадіжок особистих даних	**Кількість випадків,** *тис. од.*	**Частка від загальної кількості,** *%*
При оформленні державних пільг	394,3	32,0
При користуванні кредитними картками	365,6	29,7
Пряме викрадення особистих даних (через електронну пошту, соціальні мережі тощо)	281,4	22,9
У процесі одержання позик	99,7	8,1
У процесі взаємодії з податковими органами	89,4	7,3
Всього	1230,4	100

Джерело: складено на основі: Facts + Statistics: Identity theft and cybercrime. Insurance Information Institute. 2022. URL: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (дата звернення: 22.02.2023)

Зазвичай, під впливом методів соціальної інженерії громадяни самі відкривають зловмисникам інформацію, необхідну для проведення несанкціонованих і незаконних транзакцій. За даними Звіту ФБР, найбільш вразливими до кіберзлочинів є люди старшого віку. Так, у 2020 році в США середні втрати від одного кіберзлочину у всіх вікових групах населення становили 7076,3 дол., а у найстаршій віковій групі – 9174,3 дол., тобто на 29,7% більше (табл. 3).

В Україні, незважаючи на відсутність узагальненої статистики, ситуація з поширенням кіберзлочинів повторює загальні світові тенденції. Ще в 2017 році одна із найбільших програм-вимагачів NotPetya, розроблена на основі шкідливого програмного забезпечення (Ransomware), спочатку вразила значну кількість електронних пристроїв і комп'ютерних мереж в Україні, а потім поширилася по всьому світу, завдавши збитків підприємствам і установам як державного, так і корпоративного сектору на суму понад 10 млрд дол. США[3].

[3] OECD Digital Economy Outlook 2020. November 27, 2020. URL: https://doi.org/10.1787/bb167041-en/ (дата звернення: 17.03.2023)

Таблиця 3

Кількість випадків кіберзлочинів проти громадян та збитки від них за віковими групами населення в США у 2020 році

Вікові групи громадян	Загальна кількість випадків	Загальна сума втрат, *тис. дол. США*	Середня сума втрат на один випадок, *дол. США*
до 20 років	23186	70980,8	3061,4
20–29 років	70791	197402,2	2788,5
30–39 років	88364	492176,8	5570,0
40–49 років	91568	717161,7	7832,0
50–59 років	85967	847948,1	9863,6
старше 60 років	105301	966062,2	9174,3
Загалом	465177	3291731,8	7076,3

Джерело: складено на основі: Internet Crime Report. FBI. 2020. URL: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf (дата звернення: 10.03.2023)

На початку військових дій в Україні кількість кібератак суттєво зросла. Головними видами кіберзагроз проти органів влади, об'єктів критичної інфраструктури та корпоративного сектору стали несанкціонований збір інформації (30,4%), використання шкідливого програмного коду (24,1%) і втручання в ІК-мережі (21,9%) (табл. 4).

До того ж найбільше кібератак було здійснено на комп'ютерні мережі уряду і органів місцевої влади (22,5%), сектору безпеки та оборони (13,0%), а також фінансових установ, комерційних організацій та підприємств енергетичного сектору (табл. 5).

У 2022 році Центр кіберзахисту Національного банку України виявив майже 4,5 тис. шахрайських фішингових ресурсів, які маскувалися під державні сайти (форма шахрайства – уособлення з урядом), що на порядок більше, ніж у 2021 році. Найпоширенішим видом платіжного шахрайства стала фейкова соціальна допомога від державних і міжнародних організацій постраждалим від воєнних дій[4].

[4] Торік НБУ виявив 4,5 тисячі фішингових ресурсів, які найчастіше маскувались під держвиплати. Мінфін. 15 лютого 2023. URL: https://minfin.com.ua/ua/2023/02/15/100817382/ (дата звернення: 18.02.2023)

Таблиця 4

Види кібератак в Україні
за період з 24.02.2022 до 30.06.2022

Види кібератак	Кількість кібератак, *од.*	Питома вага в загальній кількості, *%*
Несанкціонований збір інформації	242	30,4
Впровадження шкідливого програмного коду	192	24,1
Втручання або спроби втручання в ІК-системи	174	21,9
Порушення доступності мереж	56	7,0
Інші види	132	16,6
Всього	796	100

Джерело: складено на основі: Статистика кібератак за чотири місяці війни. Державна служба спеціального зв'язку та захисту інформації України, опубліковано 30 червня 2022 р. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni (дата звернення: 01.03.2023)

Таблиця 5

Основні сектори економіки України,
на які було здійснено кібератаки за період
з 24.02.2022 до 30.06.2022

Сектори економіки	Кількість кібератак, *од.*	Питома вага в загальній кількості, *%*
Уряд і місцеві органи влади	179	22,5
Сектор безпеки та оборони	104	13,0
Фінансовий сектор	55	6,9
Комерційні організації	54	6,8
Енергетичний сектор	54	6,8
Інше	350	44,0
Всього	796	100

Джерело: складено на основі: Статистика кібератак за чотири місяці війни. Державна служба спеціального зв'язку та захисту інформації України, опубліковано 30 червня 2022 р. URL: https://www.kmu.gov.ua/news/derzhspeczvyazku-statistika-kiberatak-za-chotiri-misyaci-vijni (дата звернення: 01.03.2023)

Головним наслідком реалізації кіберзагроз є виникнення кіберризиків, які можуть порушити операційну діяльність підприємств і функціонування об'єктів критичної інфраструктури та наражають їх на значні збитки, а через наявність тісних мережевих зв'язків можуть призвести до виникнення системного ризику (*Науменкова, Міщенко*, 2014, С. 192).

Варто мати на увазі, що в перспективі кіберзагрози та кіберризики будуть дедалі частішими, а втрати – дедалі більшими. За оцінками компанії McAfee, в 2020 році в результаті реалізації кіберзагроз втрати світової економіки становили майже 1 трлн дол. США, що втричі більше порівняно з 2013 році[5]. Наприклад, середня вартість збитків лише від витоку даних у розрахунку на одне підприємство збільшилась із 3,86 млн дол. у 2020 році до 4,24 млн дол. у 2021[6]. Фахівці фондової біржі NASDAQ стверджують, що через 14 днів після того, як інформація про значну кібератаку стає публічною, середня ціна акцій на біржі знижується на 3,5%, а через пів року – ще на 3,0%[7]. За даними компанії Cybereason, у 2021 році через кібератаки 26% підприємств змушені були припинити свою діяльність[8].

Незважаючи на постійне підвищення рівня кіберзахисту та посилення кримінальної відповідальності за кіберзлочини, кіберінциденти стають дедалі більш різноманітними, оскільки кіберзлочинці активно використовують сучасні цифрові технології, зокрема, автоматизацію, штучний інтелект і машинне навчання. Так, за даними фахівців компанії McKinsey, в 2021 році основні види кіберзагроз оновилися приблизно на 80%, а шкідливі програми – майже 40%. За прогнозними розрахунками, в 2025 році збитки від кібератак можуть

[5] The Hidden Costs of Cybercrime. Report. McAfee. December, 2020. URL: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf (дата звернення: 18.02.2023)
[6] Facts + Statistics: Identity theft and cybercrime. Insurance Information Institute. 2022. URL: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (дата звернення: 22.02.2023)
[7] Global Cybersecurity Outlook 2022. Insight Report. WEF. January 2022. URL: https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf (дата звернення: 15.02.2023)
[8] Ransomware: The True Cost to Business. A Global Study on Ransomware Business Impact. Cybereason. 2022. URL: https://www.cybereason.com/ebook-ransomware-the-true-cost-to-business (дата звернення: 16.02.2023)

становити близько 10,5 трлн дол.,[9] а для України ця сума може становити 15–30 млрд дол.

Сьогодні вже йдеться про організовану кіберзлочинність – *кіберхакінг,* який став самостійною галуззю ІТ-індустрії, очолюється злочинними синдикатами (або навіть і урядами) та має у своєму розпорядження значні ресурси. Метою таких кіберзлочинів можуть бути фінансові інтереси окремих груп осіб або бажання одержати конкурентні чи геополітичні переваги, а тому технології здійснення кіберзлочинів часто випереджають технології та методи організації кіберзахисту і управління кіберризиками (*Науменкова, Міщенко,* 2015, С. 72; *Goldin et al.,* 2020).

Головними причинами посилення кіберзагроз і кіберризиків, на наш погляд, є:

– поява нових цифрових технологій та розширення сфер їх використання;

– посилення мережевих зв'язків, збільшення обсягів онлайн і мобільної взаємодії на основі використання технологій віддаленої роботи, обслуговування, е-комерції тощо;

– накопичення значних обсягів даних і розширення можливостей несанкціонованого доступу до них та інформаційних платформ, на яких вони зосереджені;

– широке використання Інтернету речей і соціальних мереж, які через недотримання вимог "кібергігієни" можуть бути потенційним джерелом кіберзагроз і ризиків;

– широке залучення в екосистемні відносини великої кількості малих і середніх підприємств та населення, які ще не мають достатнього досвіду запобігання кіберзагрозам та управління кіберризиками;

[9] Aiyer B. et al. New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers. McKinsey & Company. October 27, 2022. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers?stcr=306944F58A034922A840519AEB495476&cid=other-eml-alt-mip-mck&hlkid=b6a5856b2b094716935c909a1749aaee&hctky=13276849&hdpid=74f442d3-6737-49c1-8b01-5d1b0e77ad5d (дата звернення: 16.03.2023)

– недоліки у розробленні та використанні програмного забезпечення, проєктуванні додатків, організації та функціонуванні ІК-мереж тощо;

– використання зловмисниками для здійснення кіберзлочинів сучасних цифрових технологій та інструментів;

– недосконалість організаційних та управлінських підходів до забезпечення кіберстійкості та управління кіберризиками;

– дефіцит фахівців із кіберзахисту, нестача знань і досвіду для протидії кіберзагрозам та управління кіберризиками;

– низькі темпи стандартизації методів протидії кіберзагрозам та міжнародної співпраці зацікавлених сторін у цьому напрямі.

Наявність широкого кола чинників, які впливають на забезпечення кібербезпеки та підтримку кіберстійкості, потребує реалізації комплексного підходу до формування захисних стратегій діяльності органів влади, підприємств і громадян через створення ефективних систем кіберзахисту та управління кіберризиками.

Організація систем управління кіберстійкістю

З метою запобігання та уникнення кіберризиків система управління кіберстійкістю повинна ґрунтуватися на комплексному вирішенні технічних, технологічних, організаційних, юридичних та управлінських питань, які стосуються використання сучасного обладнання, програмного забезпечення, ІК-мереж, цифрових технологій та інструментів, а також взаємодії учасників цифрових екосистем і представників міжнародних організацій у галузі кібербезпеки.

До першочергових заходів техніко-технологічного характеру, які необхідно передбачити при формуванні та забезпеченні функціонування системи управління кіберстійкістю, на наш погляд, необхідно віднести:

- впровадження інструментів підтримки кібербезпеки в технічні та технологічні характеристики (можливості) обладнання, пристроїв, програмного забезпечення, включаючи захист від шкідливого коду в кінцевому обладнанні;
- специфікацію програмного забезпечення, в т. ч. для об’єктів Інтернету речей, з деталізацією його складових (компоненти з відк-

ритим вихідним кодом, компоненти кодової бази, інструменти сканування коду, галузеві стандарти та вимоги тощо);

- використання автономних інтелектуальних систем кіберзахисту, які на основі використання технологій штучного інтелекту та машинного навчання дозволяють забезпечити автоматичне реагування на кіберінциденти;
- формування нових IT-архітектур роботи з даними за принципом "нульової довіри" та забезпечення резервного копіювання даних у автономному режимі;
- використання безпечних методів кодування (шифрування) та систем контролю аномальної поведінки пристроїв, обладнання, співробітників і клієнтів на основі технологій поведінкової аналітики;
- стандартизацію та кодифікацію контрольно-інженерних процесів;
- створення резервних потужностей обладнання та програмно-технічних засобів;
- маркування нових пристроїв Інтернету речей та моніторинг безпеки використання вже підключених об’єктів та інші.

Головними організаційно-управлінськими заходами в системі управління кіберстійкістю повинні бути:

- розроблення, впровадження та постійний перегляд політик, процесів і стандартів забезпечення та підтримки належного рівня кіберстійкості;
- розроблення стратегій раннього виявлення кіберзагроз, планів реагування на них, планів на випадок непередбачуваних обставин і планів аварійного відновлення діяльності після збоїв з метою надання критично важливих послуг, а також забезпечення можливості відновлення діяльності до умов функціонування у стандартному режимі;
- створення надійної системи ідентифікації, контролю та управління кіберризиками з метою своєчасного виявлення ризикової події, реагування на кіберінциденти та мінімізації негативного впливу реалізації кіберзагроз;
- організація належного кіберзахисту віддалених і гібридних робочих місць;

- організація ефективного управління відносинами з третіми сторонами;
- періодичне проведення навчань і підвищення кваліфікації працівників з питань безпечної поведінки та безпечного використання цифрових ресурсів;
- розроблення та періодичне тестування сценаріїв потенційних кіберзагроз;
- підвищення рівня захисту інформації та забезпечення конфіденційності даних шляхом створення стійких репозитаріїв даних та інфраструктури для їх зберігання і оброблення, в т. ч. на загальнодоступних хмарних платформах і сервісах;
- використання ліцензованого та сертифікованого обладнання та програмного забезпечення та інші (*Подлєсна,* 2022, С. 63).

Наведений перелік складових системи управління кіберстійкістю не є вичерпним, і з часом він може змінюватися та доповнюватися. Крім того, самостійно вирішити такий широкий комплекс завдань щодо забезпечення та підтримки належного рівня кіберстійкості можуть лише великі підприємства, тоді як малі та середні підприємства потребують готових сервісів і рішень від спеціалізованих IT-компаній або використання можливостей, передбачених загальнодержавними програмами протидії кіберзагрозам.

Упродовж останніх років активного розвитку набуває індустрія кіберзахисту, потенціал якої, за даними компанії McKinsey, становить близько 2 трлн дол.[10]. Головне завдання цієї індустрії полягає в тому, щоб надати споживачам комплекс високотехнологічного обладнання, продуктів і послуг, використання яких гарантує системний захист від потенційних кіберзагроз. Водночас постачальники відповідних продуктів і послуг повинні забезпечити простоту їх упровадження та використання, що особливо важливо для малих і

[10] Aiyer B. et al. New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers. McKinsey & Company. October 27, 2022. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers?stcr=306944F58A034922A840519AEB495476&cid=other-eml-alt-mip-mck&hlkid=b6a5856b2b094716935c909a1749aaee&hctky=13276849&hdpid=74f442d3-6737-49c1-8b01-5d1b0e77ad5d (дата звернення: 16.03.2023)

середніх підприємств, а також можливість інтеграції та гнучкої адаптації в різних цифрових екосистемах.

Разом з тим ключовою передумовою забезпечення кіберстійкості підприємства, як передбачено стандартом COSO ERM:2017 "Управління ризиками підприємства – інтеграція зі стратегією та управлінням діяльністю"[11], залишається постійний контроль операційних процесів, технологій, обладнання, програм, а також розширення можливостей швидкого відновлення діяльності після збоїв.

На загальнодержавному рівні повинні бути розроблені стратегія та відповідна програма дій органів влади у законодавчій сфері, регулюванні, нагляді та контролі за станом кібербезпеки з метою попередження та своєчасного реагування на кіберзлочини (*Міщенко,* 2022, С. 187).

Національна стратегія кіберзахисту повинна передбачати ефективні заходи щодо захисту об'єктів критичної інфраструктури, Державного порталу відкритих даних, органів державної влади та населення від кіберзлочинів і шахрайства, а також систему регуляторних і наглядових заходів з метою дотриманням стандартів у сфері цифрових технологій.

Прикладами реалізації стратегічних підходів до управління кібербезпекою можуть бути прийнятий у 2022 р. в США "Закон для підвищення кібербезпеки федерального уряду та для інших цілей" (CIRCIA)[12] та Директива ЄС 2019/1024 "Про відкриті дані",[13] а прикладом галузевого підходу – загальнодержавна програма FedRAMP, яка забезпечує стандартизований підхід до оцінки безпеки, авторизації та безперервного моніторингу продуктів і послуг у галузі хмарних обчислень у США.

---

[11] Enterprise Risk Management – Integrating with Strategy and Performance. Executive Summary. Committee of Sponsoring Organizations of the Treadway Commission. COSO ERM:2017. June 2017 edition. URL: https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf (дата звернення: 14.03.2023)

[12] An Act to improve the cybersecurity of the Federal Government, and for other purposes. 117th Congress USA. 2D Session. S. 3600. URL: https://www.congress.gov/117/bills/s3600/BILLS-117s3600es.pdf (дата звернення: 18.03.2023)

[13] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. URL: https://eur-lex.europa.eu/eli/dir/2019/1024/oj (дата звернення: 18.03.2023)

Важливим етапом формування вітчизняної стратегії кіберзахисту стало ухвалення в 2017 р. Закону "Про основні засади забезпечення кібербезпеки України"[14], відповідно до якого при Державній службі спеціального зв'язку та захисту інформації України було створено Державний центр кіберзахисту, а також Центр кіберзахисту Національного банку України.

Проте окремі положення цього Закону потребують уточнення та доповнення. На наш погляд, для посилення інституційної спроможності органів влади ефективно підтримувати національну екосистему кібербезпеки з метою формування засад укоріненої стійкості та безпеки економічного розвитку України необхідно внести такі зміни.

1. Визначити терміни, обсяг, зміст, умови, засоби передачі та збереження конфіденційності інформації про кіберінциденти, яку повинні надавати об'єкти критичної інфраструктури та публічні реєстри Державному центру кіберзахисту. Обмін такою інформацією, особливо щодо кібератак і програм-вимагачів, повинен бути обов'язковим, а інформація про них, крім комерційної таємниці, повинна належати до "даних, що становлять суспільний інтерес". Наприклад, як це передбачено в США, підприємства критичної інфраструктури та фінансові компанії повідомляють Агентство з кібербезпеки та безпеки інфраструктури (CISA) про атаки програм-вимагачів упродовж 72годин, про суму сплаченого викупу – впродовж 24 годин, а про вжиті заходи реагування на кіберінциденти – в міру їх підготовки та реалізації[15].

2. У Законі або в нормативних документах Кабінету Міністрів України більш чітко викласти механізми взаємодії Державного центру кіберзахисту та об'єктів критичної інфраструктури щодо реагування на кіберінциденти, визначивши права, обов'язки та відповідальність сторін у процесі взаємодії, зокрема, необхідно передбачити санкції як до підприємств, так і до їх керівників, які не надають

[14] Про основні засади забезпечення кібербезпеки України. Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 18.03.2023)

[15] An Act to improve the cybersecurity of the Federal Government, and for other purposes. 117th Congress USA. 2D Session. S. 3600. URL: https://www.congress.gov/117/bills/s3600/BILLS-117s3600es.pdf (дата звернення: 18.03.2023)

інформацію про кіберінциденти або не виконують інші встановлені законодавством вимоги.

3. Зобов'язати публічні акціонерні товариства, які є власниками об'єктів критичної інфраструктури, обов'язково розкривати інформацію про суттєві кіберінциденти своїм інвесторам та акціонерам, передбачивши, що відповідальність за таке інформування покладається на членів ради директорів.

4. З метою вдосконалення механізмів обміну інформацією створити при Державному центрі кіберзахисту України репозитарій інформації про найбільш суттєві кіберінциденти, визначити рівні доступу до його даних та умови використання інформації окремими суб'єктами господарювання. Завдяки функціонуванню такого репозитарію підприємства та установи зможуть одержати додаткову інформацію про можливі інциденти, методи реагування на них та врегулювання наслідків від них, яку зможуть використати для оцінки потенційних кіберзагроз і розроблення адекватних заходів реагування на них у майбутньому.

На основі узагальнення наведених вище пропозицій щодо вдосконалення управління кібербезпекою розроблено структурно-логічну схему взаємодії підприємств (установ, організацій) і Державного центру кіберзахисту України в процесі обміну інформацією про кіберінциденти, яка може бути використана з метою підвищення рівня кіберстійкості до цифрових загроз і ризиків (рисунок).

Варто також зазначити, що нормативні вимоги Державного центру кібербезпеки України до об'єктів критичної інфраструктури повинні передбачати не лише систему показників звітування про кібератаки чи інші кіберзагрози, а й про здійснені заходи реагування на кіберінциденти та усунення їх наслідків. Крім того, в контексті реалізації Закону "Про основні засади забезпечення кібербезпеки України", на наш погляд, повинні бути розроблені чіткі методичні рекомендації для підприємств і установ, які б містили: стандартні архітектури організації кібербезпеки та характеристику показників оцінки її рівня; механізми управління кіберзагрозами та автоматичного реагування на кібератаки; вимоги до компетенцій визначених категорій персоналу та їхніх професійних сертифікацій; обов'язки та відповідальність керівників різних рівнів управління щодо організа-

ції, забезпечення та підтримання необхідного рівня кіберстійкості; а також порядок звітування про стан кібербезпеки.

Відповідно до Плану Відновлення України, затвердженого Національною радою з відновлення України від наслідків війни[16], в контексті реалізації національної стратегії кіберзахисту першочерговими заходами повинні бути: узгодження стандартів щодо захисту

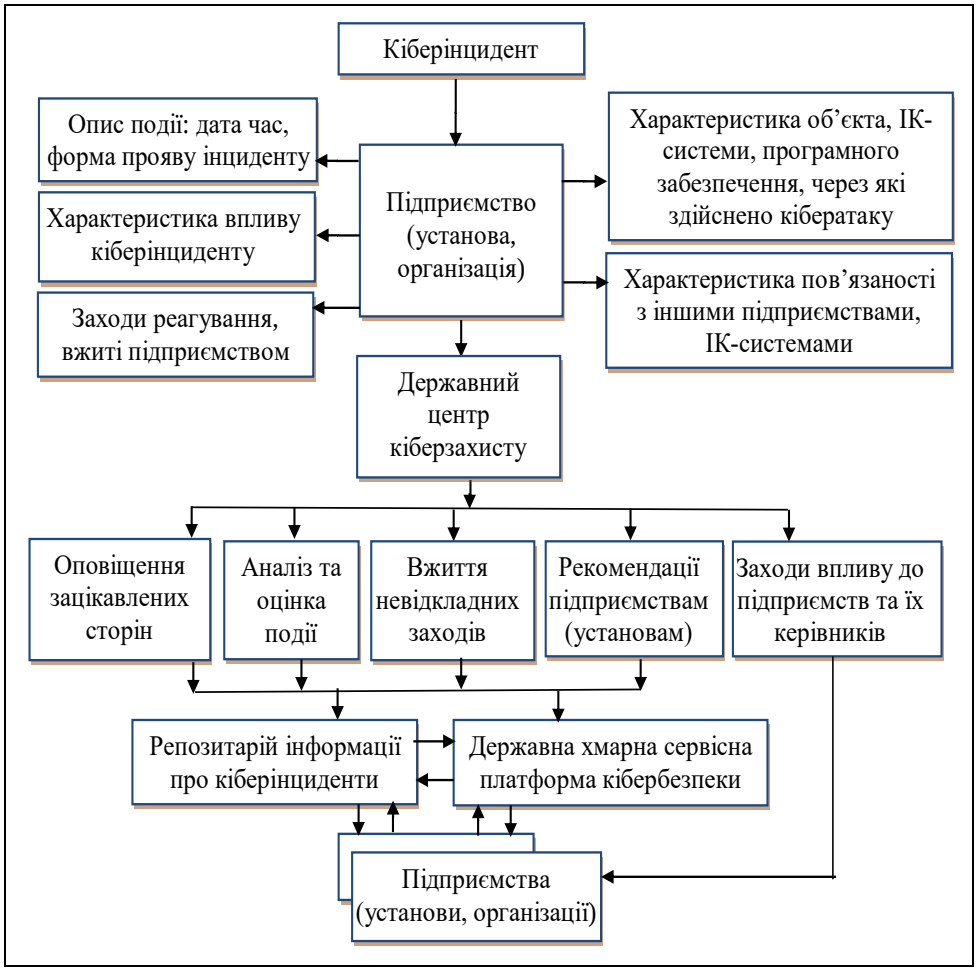

Рисунок. Схема обміну інформацією про кіберінциденти між підприємствами та Державним центром кіберзахисту України

Джерело: розроблено автором.

[16] План Відновлення України. Національна рада з відновлення України від наслідків війни. Липень 2022. URL: https://recovery.gov.ua (дата звернення: 17.03.2023)

інформації з вимогами Директиви ЄС 2019/1024 "Про відкриті дані та повторне використання інформації державного сектору";[17] гармонізація політики щодо протидії кіберзлочинам проти дітей з Європейською стратегією кращого Інтернету для дитини (BIK+)[18]; створення урядового центру очистки трафіку та протидії DDOS-атакам; використання сервісу урядового безпечного DNS та електронної пошти державних службовців; удосконалення роботи Національного центру резервування державних інформаційних ресурсів; посилення захисних можливостей загальнодержавної системи моніторингу кіберзагроз на основі використання сенсорної інфраструктури, а також розширення міжнародного співробітництва у галузі стандартизації та забезпечення кібербезпеки на всіх рівнях державного управління, що сприятиме підвищенню ефективності формування засад національно укоріненої стійкості та безпеки економічного розвитку України в умовах гібридної системи "мир-війна".

Висновки

У ході дослідження доведено, що збільшення обсягів і розширення меж використання цифрових технологій об'єктивно обумовлює виникнення кіберзагроз і наражає всіх учасників цифрових екосистем на кіберризики. Найчастіше об'єктами кібератак стають ІК-мережі, програмне забезпечення, цифрові сервіси, обладнання, цифрові активи, персональна та корпоративна пошта, облікові записи співробітників тощо. Найбільш поширеними видами кіберзагроз є фішинг, викрадення або пошкодження корпоративних і персональних даних, BEC/EAC-атаки, програми-вимагачі, зловмисна інсайдерська діяльність та інші.

Наявність широкого кола чинників, які впливають на забезпечення кібербезпеки та підтримку кіберстійкості, потребує реалізації системного підходу до формування захисних стратегій діяль-

[17] Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the re-use of public sector information. URL: https://eur-lex.europa.eu/eli/dir/2019/1024/oj (дата звернення: 18.03.2023)

[18] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+). Brussels, 11.5.2022. COM/2022/212 final. Document 52022DC0212. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:212:FIN (дата звернення: 17.03.2023)

ності органів влади, підприємств та громадян шляхом створення комплексних систем кіберзахисту, які засновані на чітких політиках, правилах і стратегіях раннього виявлення, попередження та мінімізації наслідків реалізації кіберзагроз. Важливою складовою таких систем повинен бути певний набір показників, що характеризують мінімально допустимий рівень кібербезпеки підприємства.

Розроблена у статті структурно-логічна схема взаємодії підприємств і Державного центру кіберзахисту України в процесі обміну інформацією про кіберінциденти може бути використана з метою реалізації заходів реагування та підвищення рівня кіберстійкості національної економіки.

З метою запобігання та уникнення кіберризиків система управління кіберстійкістю повинна ґрунтуватися на комплексному вирішенні технічних, технологічних, організаційних, юридичних та управлінських питань, які стосуються використання сучасного обладнання, програмного забезпечення, ІК-мереж, цифрових технологій та інструментів, а також взаємодії всіх учасників цифрових екосистем.

Продовження досліджень за обраним напрямом повинно передбачати розроблення рекомендацій щодо підвищення рівня кіберстійкості об'єктів критичної інфраструктури, створення стандартних ІТ-архітектур організації кібербезпеки, запровадження нових механізмів реагування на кібератаки, посилення відповідальності керівників підприємств і установ за організацію, забезпечення та підтримання належного рівня кіберстійкості. Подальший розвиток індустрії кіберзахисту повинен передбачати розширення спектра продуктів і послуг, які забезпечують реалізацію комплексних рішень у сфері кіберзахисту для підтримки належного рівня кіберстійкості національної економіки.

Література

1. Бандура О. В. Забезпечення комплементарності основних складових макроекономічної динаміки. *Економічна теорія.* 2020. № 4. С. 78–98. DOI: https://doi.org/10.15407/etet2020.04.078

2. Вишневський В. П. Цифрові технології та проблеми розвитку промисловості. *Економіка України*. 2022. № 1. С. 47–66. DOI: https://doi.org/10.15407/economyukr.2022.01.047

3. Гриценко А. А. Інформаційно-цифровий етап розвитку соціально-економічних систем. *Економіка України.* 2022. № 1. С. 29–46. DOI: https://doi.org/10.15407/economyukr.2022.01.029

4. Гриценко А. А. Економічні суперечності глобалізації і локалізації та їх сучасні прояви. *Економічна теорія.* 2022. № 4. С. 5–29. DOI: https://doi.org/10.15407/etet2022.04.005

5. Липов В. В. Суперечності віртуальної конкуренції як результат алгоритмізації управління на цифрових платформах: інституційний контекст. *Економічна теорія*. 2022. № 1. С. 26–44. DOI: https://doi.org/10.15407/etet2022.01.026

6. Міщенко В. І. Стратегічне управління процесами цифрової трансформації економіки. *Економіка України*. 2022. № 1. С. 67–81. DOI: https://doi.org/10.15407/economyukr.2022.01.067

7. Міщенко В. І. Цифровізація регулювання та нагляду за діяльністю фінансових установ. *Економічний простір*. 2022. 180, 182–189. DOI: https://doi.org/10.32782/2224-6282/180-30

8. Міщенко В. І., Науменкова С. В. Напрями протидії кіберзагрозам та зниження рівня кіберризиків. *Modern transformations in economics and management*. Riga, Latvia: "Baltija Publishing", 2022. P. 144–149. DOI: https://doi.org/10.30525/978-9934-26-222-7-30

9. Міщенко В. І., Науменкова С. В. Методологічні засади формування стратегії інноваційно-інвестиційного розвитку економіки України. *Причорноморські економічні студії*. 2019. № 48. С. 116–122. DOI: https://doi.org/10.32843/bses.48-19

10. Науменкова С. В., Міщенко В. І. Поняття системного ризику та підходи до визначення системно значущих банків. *Соціально-економічні проблеми сучасного періоду України*. Львів: НАН України. Ін-т регіональних досліджень 2014. Вип. 1 (105). С. 186–196.

11. Науменкова С. В., Міщенко В. І. Макропруденційні інструменти в механізмі забезпечення фінансової стабільності. *Фінанси України.* 2015. № 10. С. 53–76.

12. Подлєсна В. Г. Воєнно-економічні цикли у контексті цивілізаційного розвитку. *Економічна теорія.* 2022. № 4. С. 53–68. DOI: https://doi.org/10.15407/etet2022.04.053

13. Скрипниченко М. І. Макроекономічні оцінки і прогнози повоєнного відновлення економіки України. *Економічна теорія*. 2022. № 2. С. 29–43. DOI: https://doi.org/10.15407/etet2022.02.029

14. Філіпенко А. С. Економічна стійкість у контексті інституційної логіки. *Економічна теорія.* 2022. № 3. С. 45–56. DOI: https://doi.org/10.15407/etet2022.03.045

15. Яненкова І. Г. Світовий цифровий розвиток та нові глобальні виклики для України. *Інтернаука. Серія: Економічні науки*. 2020. № 10 (42). С. 83–95. DOI: https://doi.org/10.25313/2520-2294-2020-10-6401

16. Boehm J. et al. Cybersecurity trends: Looking over the horizon. McKinsey & Company. March 10, 2022. URL: https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity-trends-looking-over-the-horizon

17. Goldin I., Muggah R., Rohozinski R. The dark side of digitalization – and how to fix it. WEF. 2020. URL: https://www.weforum.org/agenda/2020/09/dark-side-digitalization/

18. Mishchenko S., Naumenkova S., Mishchenko V., Dorofeiev D. Innovation risk management in financial institutions. *Investment Management and Financial Innovations*. 2021. Vol. 18. Is. 1. P. 190–202. DOI: http://dx.doi.org/10.21511/imfi.18(1).2021.16

19. Mishchenko S., Naumenkova S., Mishchenko V., Ivanov V., Lysenko R. Growing discoordination between monetary and fiscal policies in Ukraine. *Banks and Bank Systems*. 2019. Vol. 14. Is. 2. P. 40–49. DOI: https://doi.org/10.21511/bbs.14(2).2019.04

20. Mishchenko V., Naumenkova S., Grytsenko A., Mishchenko S. Operational Risk Management of Using Electronic and Mobile Money. *Banks and Bank Systems*. 2022. Vol. 17. Is. 3. P. 142–157. DOI: http://dx.doi.org/10.21511/bbs.17(3).2022.12

21. Ross R., Pillitteri V., Graubart R., Bodeau D., McQuaid R. Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. NIST Special Publication 800-160. Vol. 2. Revision 1. 2021. DOI: https://doi.org/10.6028/NIST.SP.800-160v2r1

Надходження до редакції 1 березня 2023 року
Прорецензовано 10 березня 2023 року
Підписано до друку 27 березня 2023 р.

References

1. Bandura, O. (2020). Ensuring complementarity of the main components of macroeconomic dynamics. *Ekon. teor. – Economic theory*, 4, 78-98. https://doi.org/10.15407/etet2020.04.078 [in Ukrainian].

2. Vishnevsky, V. (2022). Digital technologies and problems of industrial development. *Ekon. Ukr. – Economy of Ukraine*, 1, 47-66. https://doi.org/10.15407/economyukr.2022.01.047 [in Ukrainian].

3. Gritsenko, A. (2022). Information and digital stage of development of socio-economic systems. *Ekon. Ukr. – Economy of Ukraine*, 1, 29-46. https://doi.org/10.15407/economyukr.2022.01.029 [in Ukrainian].

4. Gritsenko, A. (2022). Economic contradictions of globalization and localization and their modern manifestations. *Ekon. teor. – Economic theory*, 4, 5-29. https://doi.org/10.15407/etet2022.04.005 [in Ukrainian]

5. Lypov, V. (2022). Contradictions of virtual competition as a result of algorithmization of management on digital platforms: institutional context. *Ekon. teor. – Economic theory*, 1, 26-44. https://doi.org/10.15407/etet2022.01.026 [in Ukrainian]

6. Mishchenko, V. (2022). Strategic management of digital transformation processes of the economy. *Ekon. Ukr. – Economy of Ukraine*, 1, 67-81. https://doi.org/10.15407/economyukr.2022.01.067 [in Ukrainian].

7. Mishchenko, V. (2022). Digitalization of regulation and supervision of financial institutions. *Economic space*, 180, 182-189. https://doi.org/10.32782/2224-6282/180-30

8. Mishchenko, V., Naumenkova, S. (2022). Directions of counteraction to cyber threats and reduction of cyber risks. *Modern transformations in economics and management* (p. 144-149). Riga, Latvia: Baltija Publishing. https://doi.org/10.30525/978-9934-26-222-7-30 [in Ukrainian].

9. Mishchenko, V., Naumenkova, S. (2019). Methodological principles of forming a strategy for innovation and investment development of the Ukrainian economy. *Black Sea economic studies*, 48, 116-122. https://doi.org/10.32843/bses.48-19 [in Ukrainian].

10. Naumenkova, S., Mishchenko, V. (2014). The concept of systemic risk and approaches to the definition of systemically significant banks. *Socio-economic problems of the modern period of Ukraine,* 1 (105), 186-196. Lviv: NAS of Ukraine. Institute of Regional Studies [in Ukrainian].

11. Naumenkova, S., Mishchenko, V. (2015). Macroprudential instruments in the mechanism of ensuring financial stability. *Fin. Ukr. – Finance of Ukraine*, 10, 53-76 [in Ukrainian].

12. Podlesna, V. (2022). Military-economic cycles in the context of civilizational development. *Ekon. teor. – Economic theory*, 4, 53-68. https://doi.org/10.15407/etet2022.04.053 [in Ukrainian].

13. Skrypnychenko M. (2022). Macroeconomic estimates and forecasts of post-war economic recovery in Ukraine. *Ekon. teor. – Economic theory*, 2, 29-43. https://doi.org/10.15407/etet2022.02.029 [in Ukrainian].

14. Filipenko, A. (2022). Economic sustainability in the context of institutional logic. *Ekon. teor. – Economic theory,* 3, 45-56. https://doi.org/10.15407/etet2022.03.045 [in Ukrainian].

15. Yanenkova, I. (2020). Global digital development and new global challenges for Ukraine. *Internauka, Ser.: Economic Sciences*, 10 (42), 83-95. https://doi.org/10.25313/2520-2294-2020-10-6401 [in Ukrainian].

16. Boehm J. et al. (March 10, 2022). Cybersecurity trends: Looking over the horizon. McKinsey & Company. Retrieved from https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity-trends-looking-over-the-horizon

17. Goldin, I., Muggah, R., Rohozinski, R. (2020). The dark side of digitalization – and how to fix it. WEF. Retrieved from https://www.weforum.org/agenda/2020/09/dark-side-digitalization/

18. Mishchenko, S., Naumenkova, S., Mishchenko, V., Dorofeiev, D. (2021). Innovation risk management in financial institutions. *Investment Management and Financial Innovations*, 18(1), 190-202. http://dx.doi.org/10.21511/imfi.18(1).2021.16

19. Mishchenko, S., Naumenkova, S., Mishchenko, V., Ivanov, V., Lysenko, R. (2019). Growing discoordination between monetary and fiscal policies in Ukraine. Banks and Bank Systems, 14(2), 40-49. https://doi.org/10.21511/bbs.14(2).2019.04

20. Mishchenko, V., Naumenkova, S., Grytsenko, A., Mishchenko, S. (2022). Operational Risk Management of Using Electronic and Mobile Money. *Banks and Bank Systems,* 1 (17), 142-157. http://dx.doi.org/10.21511/bbs.17(3).2022.12

21. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., McQuaid, R. (2021). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. *NIST Special Publication* 800-160, 2 (1). https://doi.org/10.6028/NIST.SP.800-160v2r1

Received on March 1, 2023
Reviewed March 10, 2023
Signed before printing March 27, 2023