# ДОСВІД ЄС ЩОДО РОЗРОБКИ ТА ВПРОВАДЖЕННЯ НАЦІОНАЛЬНОЇ СТРАТЕГІЇ КІБЕРСТІЙКОСТІ ФІНАНСОВОГО СЕКТОРУ[1]

# THE EU EXPERIENCE ON DEVELOPING AND IMPLEMENTING A NATIONAL CYBER RESILIENCE STRATEGY FOR THE FINANCIAL SECTOR

*Зважаючи на постійний технологічний прогрес і зростання кількості злочинних схем, забезпечення кіберстійкості фінансового сектору стає пріоритетним завданням регулюючих органів. Протягом останніх років було розроблено багато міжнародних, європейських і національних нормативних актів і галузевих стандартів у сфері інформаційної безпеки та кіберзахисту. В статті проведено порівняльний аналіз основних здобутків у сфері забезпечення кіберстійкості фінансової системи у країнах Європейського Союзу та Україні за такими складовими: загальні положення стратегії кібербезпеки, захист від кіберзагроз, реакція на кіберінциденти та розвиток системи кібербезпеки. Враховуючи наявні здобутки у розбудові національної системи кібербезпеки, подальшого удосконалення потребують процедури реагування на кіберінциденти, окремі компоненти національної системи кібербезпеки, пруденційні вимоги до кібербезпеки фінансових установ.*

**Ключові слова:** *кіберстійкість, кіберризики, кіберінциденти, регулювання, захист інформації, інформаційна безпека, фінансова система.*

*Given the evolving landscape of technological advancements and the proliferation of sophisticated criminal activities, fortifying the cyber resilience of the financial sector stands as a paramount obligation for regulatory bodies. In recent years, numerous international, European, and national regulatory frameworks, as well as industry standards, have emerged to address the domains of information security and cyber protection. Specialized European organizations and the national governments of European countries have made significant strides in developing effective legislation to combat cybercrime, conducting informational and educational campaigns for personal and corporate cyber protection, and seeking mechanisms to bolster the cyber resilience of economic entities. Considering this, the article aims to conduct a comparative analysis of the European and Ukrainian approaches to formulating and executing national strategies focused on enhancing the cyber resilience of the financial system. The article delves into the analysis of cyber incidents and data breaches within the financial sector. It performs a comparative assessment of the primary achievements in ensuring the cyber stability of the financial system across European Union countries and Ukraine. This evaluation encompasses key components: the foundational principles of cyber security strategy, defenses against cyber threats, responses to cyber incidents, and the evolution of cyber security systems. Recognizing the progress achieved in the development of national cyber security systems, the authors ascertain that the response procedures for cyber incidents, individual elements within the national cyber security framework, and the regulatory requirements for the cyber security of financial institutions necessitate further enhancement. These enhancements should align with the evolving cyber landscape, ensuring adaptability and robustness in the face of emerging threats and technological advancements. This involves continuous updates to defensive measures against cyber threats and the augmentation of response protocols to effectively counter evolving attack methodologies.*

**Key words:** *cyber resilience, cyber risks, cyber incidents, regulation, information protection, information security, financial system.*

УДК 336.02:004.056

DOI: https://doi.org/10.32782/dees.8-21

**Боженко В.В.**[2]
к.е.н., доцент,
Сумський державний університет
**Пахненко О.М.**[3]
к.е.н., доцент,
Сумський державний університет
**Койбічук В.В.**[4]
к.е.н., доцент,
Сумський державний університет

**Bozhenko Victoria**
Sumy State University
**Pakhnenko Olena**
Sumy State University
**Koybichuk Vitalia**
Sumy State University

**Постановка проблеми.** Стрімка цифрова трансформація бізнес-процесів фінансових установ, складна екосистема ланцюгів постачання та акумулювання значного масиву персональних та фінансових даних призводить до того, що фінансові установи є головними цілями для кіберзлочинців. За даними компанії IBM про публічно розкриті кіберзлочини протягом 2018–2022 років фінансовий сектор був і залишається найбільш вразливою сферою діяльності до кіберзлочинності [1].

Фінансові установи, які пов'язані один з одним через платіжні та операційні мережі, можуть наражатися на загрозу численних кібератак. У випадку компрометації інформаційної та кібернетичної безпеки однієї фінансової установи, кіберінцидент може призвести до ланцюгової реакції та зараження шкідливим програмним забезпеченням або іншими небезпеками інших суб'єктів господарювання. Фінансове зараження центрального банку може мати масштабні наслідки, які ймовірно спричиняють порушення системи електронних платежів та обмежать доступ до фінансових ресурсів держави. Виходячи з цього, визначення стратегічних векторів забезпечення стійкості всіх учасників фінансової системи до кіберзагроз має вирішальне значення для недопущення значних фінансових збитків, витоку конфіденційних даних та збереження довіри до сфери фінансових послуг з боку основних стейкхолдерів.

**Аналіз останніх досліджень і публікацій.** Питання кіберстійкості фінансового сектору є фокусом багатьох сучасних досліджень вітчиз-

[1] Роботу виконано в рамках проєкту Жан Моне (Модуль) «Практики ЄС щодо захисту фінансової системи від кіберзагроз» (EU_PITCH).

[2] ORCID: https://orcid.org/0000-0002-9435-0065

[3] ORCID: https://orcid.org/0000-0002-4703-4078

[4] ORCID: https://orcid.org/0000-0002-3540-7922

няних та зарубіжних науковців [2–7]. Одні з найбільш концептуальних досліджень проводить Дюпон Б., зокрема ним обґрунтована потреба в кіберстійкості у фінансовому секторі, досліджено п'ять вимірів організаційної стійкості та проаналізовано типи інституційних підходів, які використовуються для сприяння кіберстійкості у фінансовому секторі [2]. Разом зі співавторами Дюпон Б. досліджує організаційну компоненту кіберстійкості та напруги (складнощі), пов'язані з її впровадженням: напругу визначення, напругу середовища, внутрішню напругу та нормативну напругу [3].

Серед вітчизняних дослідників досить частим об'єктом аналізу виступає кіберстійкість банків. Криклій О.А. на основі узагальнення сутнісних характеристик кіберстійкості банку пропонує модель механізму забезпечення кіберстійкості банків України [5]. Білошапка В., Охрименко І. та Чуб П. аналізують ініціативи центрального банку щодо посилення регуляторного контролю за кіберзахистом та інформаційною безпекою банків в умовах інтенсивного розвитку цифрового фінансового простору [6]. Шлапак А. розглядає роль фінансових установ у відсіюванні недостовірної інформації, попередженні кібершахрайств та інших зловживань [7].

Крім того, різні аспекти кіберстійкості фінансового сектору є об'єктом уваги та наукових досліджень багатьох міжнародних установ та організацій, таких як Світовий банк, Світовий економічний форум, Фонд Карнеґі за міжнародний мир та інших. Прикладом є представлена в публікації Світового банку методологія впровадження в дію Керівництва з кіберстійкості для суб'єктів інфраструктури фінансового ринку [8].

Вагомий внесок у розробку ефективного законодавства для боротьби з кіберзлочинністю, проведення інформаційно-просвітницьких та освітніх кампаній щодо персонального та корпоративного захисту в кіберпросторі, а також пошуку механізмів підвищення кіберстійкості економічних суб'єктів здійснюється європейськими профільними організаціями та національними урядами європейських країн.

Зважаючи на це, **метою статті** є проведення порівняльного аналізу європейських та вітчизняної практики затвердження та реалізації національної стратегії, спрямованої на забезпечення кіберстійкості фінансової системи.

**Виклад основного матеріалу дослідження.** Термін кіберстійкість означає здатність захищати електронні дані та інформаційні системи фінансових установ від кібератак, а також швидко відновлювати бізнес-операції у разі кіберінциденту [9]. Статистичні дані засвідчують збільшення кількості кібератак на фінансові установи. Рекордним за кількістю кіберінцидентів у фінансовому секторі є 2022 рік, коли було зафіксовано 2527 інцидентів (рис. 1).

Кіберінциденти, що супроводжуються витоком даних, завдають суттєвих збитків світовій економіці. У 2022 році середня вартість одного витоку даних (загалом по світу і усім видам діяльності) склала 4,35 млн доларів. Фінансовий сектор за цим показником є одним із «лідерів», середній обсяг збитків за кіберінцидентами у фінансовому секторі в 2022 році становив 6 млн доларів, що майже в 1,4 рази більше середньосвітового показника. Вищий рівень збитків (10,1 млн доларів на один кіберінцидент) був лише у сфері охорони здоров'я [11].

Частота та складність кібератак у фінансовому секторі потребують посилення регуляторного нагляду за кіберризиками. Рівень кіберстійкості

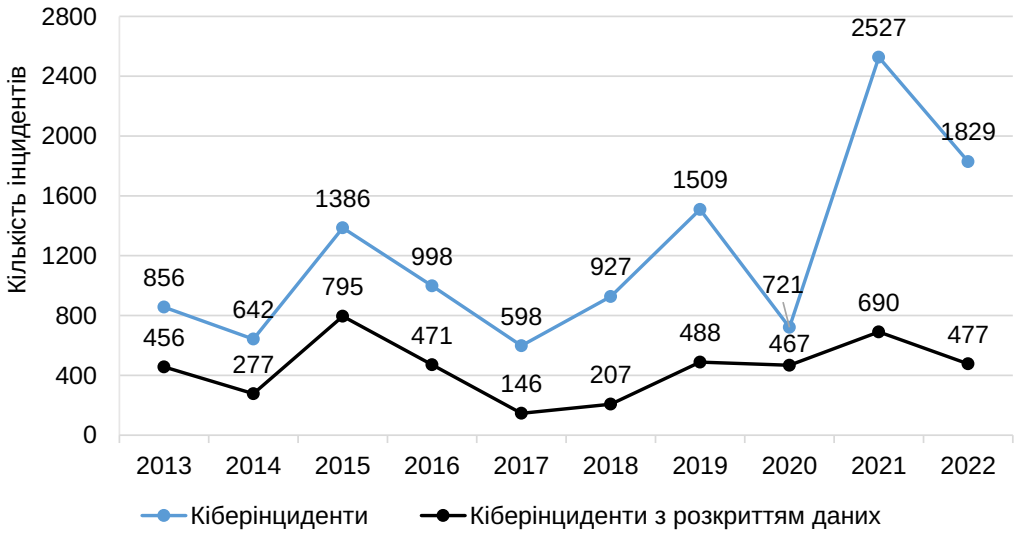


**Рис. 1. Глобальні показники кіберінцидентів у фінансовому секторі протягом 2013–2022 рр.**

*Джерело: [10]*

фінансової системи залежить від законодавчого регулювання, розробки та впровадження політики інформаційної безпеки фінансовими установами, а також від комплексу державних ініціатив щодо підвищення рівня обізнаності громадськості про базові правила кібербезпеки та кібергігієни.

Підвищення кіберстійкості фінансової системи є безперервним процесом, який включає кілька основних етапів:

– захист від кіберзагроз (виявлення кіберврразливостей у фінансовій системі; оцінка рівня готовності протистояти кіберзагрозам; проведення симулятивних тренувань щодо реагування на кібератаки; затвердження базових заходів безпеки для всіх або окремих учасників фінансової системи та інші заходи);

– реакція на кіберінциденти (пошук методів виявлення вторгнень у діяльність учасників фінансової системи; затвердження чітких процедур реагування на кіберінциденти; розробка сценаріїв відновлення сталості і надійності функціонування інформаційно-комунікаційних та технологічних систем учасників фінансової системи тощо);

– розвиток системи кібербезпеки (обмін інформацією про кіберінциденти, затвердження програм підвищення кваліфікації та навчання працівників у сфері кібербезпеки; проведення регулярних просвітницьких заходів щодо підвищення рівня цифрової грамотності та кібергігієни громадян країни; розвиток програм державно-приватного партнерства та інші заходи).

У таблиці 1 наведено порівняльний аналіз основних здобутків у сфері забезпечення кіберстійкості фінансової системи у країнах Європейського Союзу та України у розрізі вище виокремлених етапів (захист від кіберзагроз, реакція на кіберінциденти, розвиток системи кібербезпеки). Відзначимо, що систематизація здобутків учасників фінансової системи у сфері кібербезпеки, які функціонують на території Європейського Союзу, передбачала аналіз європейських і національних нормативних актів і галузевих стандартів у сфері інформаційної безпеки та кіберзахисту.

Порівняльний аналіз складових кіберстійкості дозволяє стверджувати про європейське наслідування Національним банком України та іншими регулюючими та контролюючими органами України кращих практик у сфері кібербезпеки. І цьому є закономірне пояснення, оскільки протягом останнього десятиліття Європейський Союз розробив та системно оновлює правові рамки забезпечення загального рівня кібербезпеки, об'єднує зусилля

Таблиця 1

**Порівняльний аналіз основних здобутків у сфері забезпечення кіберстійкості фінансової системи у країнах Європейського Союзу та Україні**

| Складові кіберстійкості | | Країни ЄС | Україна |
|---|---|---|---|
| Загальні положення | Наявність затвердженої національної стратегії кібербезпеки | + | + |
| | Фінансові установи включені до об'єктів критичної інфраструктури | + | + |
| Захист від кіберзагроз | Наявність вказівок/рекомендацій щодо базових заходів інформаційної безпеки та кіберзахисту для учасників фінансової системи | + | + |
| | Проведення фінансовими установами самооцінки стану інформаційної безпеки та кіберзахисту | + | + |
| | Контроль за дотриманням заходів інформаційної безпеки та кіберзахисту | + | + |
| | Відокремлення в архітектурі операційного ризику «кіберризику» | + | + |
| | Затверджені пруденційні вимоги до кібербезпеки фінансових установ | + | - |
| | Обов'язкове проведення аудиту інформаційної безпеки фінансових установ | + | + |
| | Симуляція контрольованих кібератак для визначення кіберврразливостей фінансових установ | + | - |
| Реакція на кіберінциденти | Затверджена процедура реагування на кіберзагрози | + | + |
| | Встановлені терміни реагування на кіберінциденти та кібератаки | + | - |
| | Затверджена процедура щодо обов'язкового обміну кіберінформацією та розвідданими між фінансовими установами | + | - |
| Розвиток системи кібербезпеки | Наявність комплексних програм навчання та /або підвищення кваліфікації працівників у сфері кібербезпеки | + | + |
| | Наявність безкоштовних базових тренінгів з кібербезпеки для громадян країни | + | + |
| | Наявність схвалених та профінансованих дослідницьких проєктів, орієнтованих на вивчення питання кібербезпеки | + | - |
| | Наявність кластерів кібербезпеки | + | + |

*Джерело: авторська розробка*

практиків, етичних хакерів і національних регуляторів для пошуку нових методів та інструментів протидії кіберзагрозам у фінансовому секторі економіки, а також сформував розгалуджену мережу інституцій для організації кібербезпеки.

Важливим компонентом у створенні умов для безпечного функціонування кіберпростору в рамках країни є розробка та затвердження національної стратегії кібербезпеки, в якій мають бути визначені основні пріоритети, цілі та завдання забезпечення кібербезпеки. Станом на 2017 рік всі країни-члени Європейського Союзу затвердили власні національні стратегії кібербезпеки. Стратегія кібербезпеки України була вперше затверджена у 2016 році, проте з урахуванням нових кіберзагроз та викликів у сфері інформаційної безпеки об'єктів критичної інфраструктури у 2021 році була ухвалена нова Стратегія [12]. Фінансові установи віднесені до об'єктів критичної інфраструктури як в Україні, так і в країнах ЄС. Зокрема, у 2022 році Європейський Союз включив сферу фінансових та платіжних послуг до об'єктів критичної інфраструктури, до яких належать фінансово-кредитні установи, оператори електронних торгових майданчиків та центральні контрагенти (Директива Європейського Союзу щодо стійкості критичних об'єктів) [13].

**Висновки.** Процес підвищення кіберстійкості фінансової системи включає декілька етапів: захист від кіберзагроз, реакція на кіберінциденти та розвиток національної системи кібербезпеки. За період реалізації Стратегії кібербезпеки України з 2016 року було забезпечено суттєвий прогрес у становленні та розвитку національної системи кібербезпеки. Зокрема, було удосконалено нормативне забезпечення з питань кіберзахисту об'єктів критичної інформаційної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту. Також відбулася розбудова організаційної структури національної системи кібезбезпеки. Втім, все ще потребують доопрацювання та удосконалення процедури реагування на кіберінциденти, окремі компоненти національної системи кібербезпеки, вимоги до кібербезпеки фінансових установ. Незалежно від рівня кіберстійкості фінансової системи, повністю запобігти кібератакам неможливо. Окрім заходів на національному рівні, усі фінансові установи повинні розробляти та реалізовувати власні стратегії забезпечення кібербезпеки для того, щоб ефективно протистояти кібератакам, адаптуватися до них і швидко відновлюватися, зберігаючи при цьому безперервність роботи.

**БІБЛІОГРАФІЧНИЙ СПИСОК:**

1. X-Force Threat Intelligence Index 2023. IBM Security. 2023. URL: https://www.ibm.com/reports/threat-intelligence (дата звернення: 06.10.2023).

2. Dupont B. The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*. 2019. Vol. 5, issue 1. P. 1–17. DOI: 10.1093/cybsec/tyz013

3. Dupont B., Shearing C., Bernier M., Leukfeldt R. The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security.* 2023. Vol. 132, 103372. DOI: 10.1016/j.cose.2023.103372

4. Li Yu., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 2021. Vol. 7. P. 8176–8186. DOI: 10.1016/j.egyr.2021.08.126

5. Криклій О.А. Теорія та практика забезпечення кіберстійкості банків. *Ефективна економіка*. 2020. № 10. URL: http://www.economy.nayka.com.ua/?op=1&z=8248 (дата звернення: 06.10.2023). DOI: 10.32702/2307-2105-2020.10.50

6. Білошапка В., Охрименко І., Чуб П. Регуляторний контроль за інформаційною та кібербезпекою банків в умовах інтенсивної цифровізації. *Наука і техніка сьогодні*. 2022. № 14(14). С. 96–109. DOI: 10.52058/2786-6025-2022-14(14)-96-109

7. Шлапак А. Наглядовий потенціал фінансових установ у протидії кіберзлочинам та інформаційним асиметріям в умовах зростання ролі FINTECH і BIG TECHS на цифровізованих ринках капіталу. *Вісник Хмельницького національного університету.* 2022. № 2(2). С. 273–280. DOI: 10.31891/2307-5740-2022-304-2(2)-43

8. Cyber Resilience for Financial Market Infrastructures. The World Bank. November 2019. URL: https://thedocs.worldbank.org/en/doc/189821576699037673-0130022019/original/FIGIECBOperationalCyberFinalWeb1213.pdf (дата звернення: 06.10.2023).

9. What is cyber resilience? European Central Bank. URL: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html (дата звернення: 06.10.2023).

10. Petrosyan A. Global number of cyber attacks in financial sector 2013-2022. Statista. 2023. URL: https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/ (дата звернення: 06.10.2023).

11. Petrosyan A. Cyber crime: all-time biggest online data breaches 2023. Statista. 2023. URL: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/ (дата звернення: 06.10.2023).

12. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 06.10.2023).

13. The Critical Entities Resilience Directive: Directive EU 2022/2557. European Parliament. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (дата звернення: 06.10.2023).

**REFERENCES:**

1. IBM Security (2023). X-Force Threat Intelligence Index 2023. Available at: https://www.ibm.com/reports/threat-intelligence (accessed October 6, 2023).

2. Dupont B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, vol. 5, issue 1, pp. 1–17. DOI: 10.1093/cybsec/tyz013

3. Dupont B., Shearing C., Bernier M., Leukfeldt R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security,* vol. 132, 103372. DOI: 10.1016/j.cose.2023.103372

4. Li Yu., Liu Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, vol. 7, pp. 8176–8186. DOI: 10.1016/j.egyr.2021.08.126.

5. Kryklii O. (2020). Teoriya ta praktyka zabezpechennya kiberstiykosti bankiv [Theory and practice of ensuring cyber-resilience of banks]. *Efektyvna ekonomika*, vol. 10. Available at: http://www.economy.nayka.com.ua/?op=1&z=8248 (accessed October 6, 2023). DOI: 10.32702/2307-2105-2020.10.50 [in Ukrainian]

6. Biloshapka V., Okhrymenko I., Chub P. (2022). Rehulyatornyy kontrol za informatsiynoyu ta kiberbezpekoyu bankiv v umovakh intensyvnoyi tsyfrovizatsiyi [Regulatory control of information and cyber security of banks in the conditions of intensive digitalization]. *Science and Technology Today*, vol. 14(14), pp. 96–109. DOI: 10.52058/2786-6025-2022-14(14)-96-109 [in Ukrainian]

7. Shlapak A. (2022). Nahlyadovyy potentsial finansovykh ustanov u protydiyi kiberzlochynam ta informatsiynym asymetriyam v umovakh zrostannya roli FINTECH i BIG TECHS na tsyfrovizovanykh rynkakh kapitalu [Supervisory capacity of financial institutions in countering cybercrime and information asymmetries in the conditions of the growth of the role of FINTECH and BIG TECHS in the digitalized international capital markets]. *Visnyk Khmel'nyts'koho natsional'noho universytetu,* vol. 2(2), pp. 273–280. DOI: 10.31891/2307-5740-2022-304-2(2)-43 [in Ukrainian]

8. Cyber Resilience for Financial Market Infrastructures. The World Bank. November 2019. Available at: https://thedocs.worldbank.org/en/doc/189821576699037673-0130022019/original/FIGIECBOperationalCyberFinalWeb1213.pdf (accessed October 6, 2023).

9. European Central Bank (2023). What is cyber resilience? Available at: https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html (accessed October 6, 2023).

10. Petrosyan A. (2023). Global number of cyber attacks in financial sector 2013-2022. Statista. Available at: https://www.statista.com/statistics/1310985/number-of-cyber-incidents-in-financial-industry-worldwide/ (accessed October 6, 2023).

11. Petrosyan A. (2023). Cyber crime: all-time biggest online data breaches 2023. Statista. Available at: https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/ (accessed October 6, 2023).

12. Pro rishennya Rady natsionalnoyi bezpeky i oborony Ukrayiny vid 14 travnya 2021 roku «Pro Stratehiyu kiberbezpeky Ukrayiny». Ukaz Prezydenta Ukrayiny [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 “On the Cybersecurity Strategy of Ukraine”. Decree of the President of Ukraine]. Available at: https://zakon.rada.gov.ua/laws/show/447/2021#Text (accessed October 6, 2023) [in Ukrainian]

13. The Critical Entities Resilience Directive: Directive EU 2022/2557. European Parliament. Available at: https://eur-lex.europa.eu/eli/dir/2022/2557/oj (accessed October 6, 2023)