Міністерство освіти і науки України

Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

Навчально-науковий інститут фінансів, економіки,
управління та права
Кафедра фінансів, банківського бізнесу та оподаткування

ЕКОНОМІЧНА БЕЗПЕКА: ДЕРЖАВА, РЕГІОН, ПІДПРИЄМСТВО

Матеріали IX Міжнародної
науково-практичної конференції

15 травня 2025 р.

Полтава
2025

УДК 336.71:343.326

Вовченко Оксана Сергіївна,
кандидат економічних наук, доцент
Грищук Вероніка В'ячеславівна,
студентка
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

КІБЕРЗАГРОЗИ В БАНКІВСЬКОМУ СЕКТОРІ: СУЧАСНІ ВИКЛИКИ ТА МЕТОДИ ПРОТИДІЇ

У добу цифрових трансформацій та глобалізації фінансових ринків банківський сектор відіграє ключову роль у забезпеченні функціонування національної економіки. Саме тому стабільність, безпечність та стійкість фінансових установ є одними зі складових економічної безпеки держави. З огляду на високу концентрацію конфіденційних даних, фінансових потоків і критичних інформаційних систем, банки залишаються пріоритетними об'єктами для кіберзлочинців.

Вивчення кіберзагроз у банківській сфері є актуальним з кількох ключових причин. По-перше, масштаби цифровізації фінансових послуг щороку зростають. За даними НБУ, частка онлайн-операцій у загальній структурі банківських транзакцій сягнула понад 80 % у 2023 році. По-друге, фінансові установи дедалі частіше інтегруються у глобальні інформаційні ланцюги, що підвищує ризик зовнішніх атак. По-третє, порушення кібербезпеки може спричинити серйозні репутаційні втрати, фінансові збитки, а в окремих випадках – системні ризики для всієї банківської системи.

Зокрема, фішинг залишається найбільш поширеним методом соціальної інженерії, який зловмисники використовують для отримання доступу до банківських систем або персональних даних клієнтів. DDoS-атаки мають на меті паралізувати функціонування електронних систем,

створити хаос у роботі онлайн-банкінгу. Malware-атаки орієнтовані на отримання неправомірного контролю над IT-інфраструктурою установи.

Таблиця 1

Динаміка кіберінцидентів у фінансовому секторі України за 2021–2024 роки

Рік	Кількість інцидентів	Найпоширеніші типи атак
2021	480	Фішинг, трояни
2022	620	Ransomware, DDoS
2023	890	Цілеспрямовані атаки на інфраструктуру
2024	1030	Комбінації різних видів атак

Джерело: узагальнено автором за даними [1]

Крім того, кіберзагрози є динамічним явищем: з розвитком технологій змінюються і підходи зловмисників. Відтак, виникає потреба у постійному моніторингу, аналізі та прогнозуванні нових типів атак, удосконаленні засобів захисту та формуванні адаптивної кіберстратегії банківських установ.

Із початком повномасштабної агресії проти України у 2022 році спектр кіберзагроз значно розширився. Хакерські угруповання, пов’язані з державою-агресором, активізували діяльність, зокрема проти об’єктів фінансової інфраструктури. У цьому контексті з’явилися нові виклики, серед яких варто відзначити:

1) Advanced Persistent Threats (APT) – цілеспрямовані атаки, які можуть залишатися непоміченими протягом тривалого часу;

2) Wiper-атаки – деструктивне програмне забезпечення, що видаляє або шифрує дані без можливості відновлення;

3) Supply Chain Attacks – ураження слабких ланок в ланцюзі партнерських IT-систем банку.

Аналіз динаміки основних показників кіберзагроз у банківському секторі України за період 2022–2024 років свідчить про стійку тенденцію до зростання кіберінцидентів як за кількістю, так і за масштабами фінансових втрат.

Таблиця 2

Динаміка кіберзагроз у банківському секторі України за 2022–2024 роки

Показник	2022	2023	2024
Кількість інцидентів, шт.	218 000	272 000	310 000
Загальна сума втрат, млн.грн.	481	833	102
Частка шахрайства через Інтернет, %	78	83	85
Частка інцидентів через соціальну інженерію, %	53	80	82

Джерело: узагальнено автором за даними [1, 2]

В умовах воєнного стану важливість забезпечення кіберстійкості набуває додаткового стратегічного значення. Адже банківські установи не лише забезпечують фінансове обслуговування громадян і бізнесу, а й виступають важливою складовою державної економічної стійкості. З огляду на стрімке зростання кіберризиків, НБУ виступає провідним регулятором у сфері формування політики кіберзахисту в банківському секторі. У 2022–2024 роках ним було запроваджено низку нормативних документів та ініціатив, спрямованих на підвищення рівня кіберстійкості фінансових установ. Зокрема, Постанова НБУ №95 [3] встановлює мінімальні вимоги до інформаційної безпеки та зобов'язує банки здійснювати регулярні оцінки вразливостей, проводити незалежні тестування на проникнення (penetration testing), а також впроваджувати системи виявлення інцидентів безпеки (SIEM, IDS/IPS).

Окремої уваги заслуговує діяльність Центру реагування на кіберінциденти FinCERT, створеного при НБУ. Цей центр виконує координаційну функцію між банками, технічними

провайдерами та державними структурами (СБУ, Держспецзв'язок), здійснює аналіз поточних кіберзагроз, поширює сигнали попередження (alerts) та забезпечує обмін оперативною інформацією щодо виявлених вразливостей.

Самі комерційні банки, відповідно до регуляторних вимог, також активно реалізовують інформаційно-технологічні заходи, серед яких: розгортання систем багатофакторної автентифікації для клієнтів і персоналу; впровадження кіберплатформ управління ризиками; резервне копіювання та сегментація мережевої інфраструктури для зменшення наслідків потенційного вторгнення; автоматизований моніторинг журналів подій та аномалій у транзакціях.

Таким чином, протидія кіберзагрозам у банківському секторі є важливою складовою сучасної економічної безпеки. Успішне подолання викликів можливе лише за умов системного підходу, що об’єднує технічні, організаційні, правові та освітні інструменти. Серед напрямів подальшого підвищення кіберстійкості українських банків можна визначити: впровадження адаптивних моделей ризик-менеджменту, заснованих на аналізі великих даних (Big Data); розвиток кадрового потенціалу у сфері кіберзахисту, включаючи сертифікацію фахівців за міжнародними стандартами (CISSP, CEH, ISO 27001); застосування штучного інтелекту та машинного навчання для виявлення нових атипових атак; участь у спільних національних та міжнародних навчаннях з кібербезпеки (наприклад, CyberCoalition, Cyber Europe).

Література

1. Річний звіт Національного банку України за 2023 рік. URL: https://bank.gov.ua/ua/news/all/richniy-zvit-natsionalnogo-banku-ukrayini-za-2023-rik

2. Financial Services Information Sharing and Analysis Center (FS-ISAC). Cyber Intelligence Report Q4 2023. FS-ISAC, 2024. 15 с. URL:

https://www.fsisac.com/hubfs/Knowledge/NavigatingCyber/2024/FSISAC-NavCyber24-Report.pdf

3. Про підвищення рівня захищеності інформаційних систем банків. Постанова Правління Національного банку України №95 від 09 трав. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/v0095500-22#Text

УДК 338:004.7.056

Глушко Аліна Дмитрівна,
кандидат економічних наук, доцент
Тесля Олександр Дмитрович, Лукаш Ілля Миколайович,
студенти
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

ІНФОРМАЦІЙНА БЕЗПЕКА ПІДПРИЄМСТВА ЯК БАЗИС ЙОГО ЕКОНОМІЧНОЇ СТІЙКОСТІ

В умовах цифровізації економіки та глобального інформаційного середовища питання забезпечення інформаційної безпеки набуває критично важливого значення для підприємств усіх галузей. Сучасні компанії стикаються з безпрецедентним зростанням кіберзагроз, витоків даних, шахрайських дій та інших інформаційних ризиків, які безпосередньо впливають не лише на операційну діяльність, а й на загальну фінансову стабільність та конкурентоспроможність. Інформаційна безпека сьогодні розглядається не лише як технічна складова IT-інфраструктури, а як стратегічний ресурс, що визначає здатність підприємства адаптуватися до змін, реагувати на зовнішні загрози та зберігати свою економічну сталість у довгостроковій перспективі.

Комплексне управління інформаційною безпекою, що поєднує технічні, організаційні та правові інструменти,