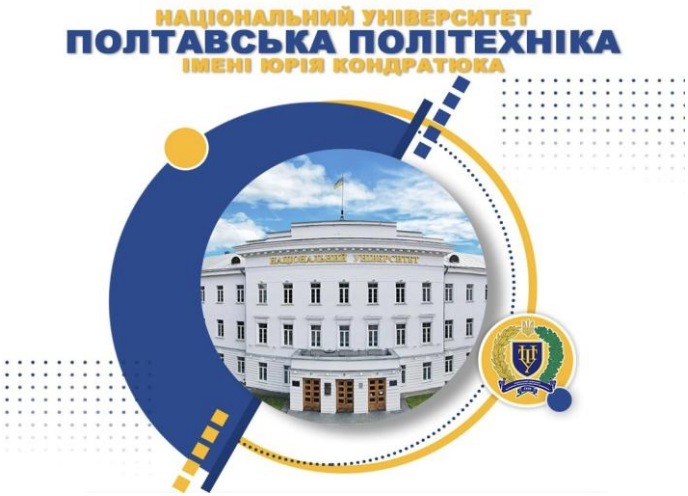
Міністерство освіти і науки України

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 336.32

Худолій Юлія Сергіївна,
кандидат економічних наук, доцент
Білько Анастасія Вікторівна, Чорнобель Карина Олексіївна,
студентки
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

КІБЕРБЕЗПЕКА В БАНКІВСЬКІЙ СФЕРІ ЯК СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ В УКРАЇНІ В КОНТЕКСТІ ЄВРОІНТЕГРАЦІЇ

В теперішній час питання економічної безпеки – дуже важливі, бо від них залежить геополітичне майбутнє країни, стан національної економіки, соціально-економічний достаток громадян. Можна казати, що вирішення окреслених питань значною мірою залежить від ІТ-сфери, оскільки в постіндустріальному суспільстві інформаційні технології заполонили всі сфери життєдіяльності людини, а також й економічну. Інформаційно-телекомунікаційні системи потребують захисту через те, що ми маємо швидкий розвиток інформаційних технологій. Але інформаційні технології також створюють можливості для низки правопорушень та зловживань. Кіберзлочинам останнім часом піддаються не тільки фізичні особи, а також підприємства. Отже, країни не можуть стверджувати, що в них є власна економічна безпека, якщо вона не захищена у кіберпросторі [5].

Кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Відповідно до законодавства, держава гарантує безпеку громадян України як на її території, так і за кордоном. Громадяни, організації та об'єднання також є суб'єктами безпеки з визначеними правами й обов'язками. Об'єктами безпеки виступають особистість, суспільство, держава, а також підприємства та установи. Для забезпечення безпеки створюється система правових норм, відповідні державні органи та механізми контролю. Економічна безпека є ключовим національним пріоритетом і розглядається як складова національної безпеки. Вона забезпечує стійкий розвиток, захист економічних інтересів і складається з економічної незалежності, стабільності національної економіки та здатності до саморозвитку [2].

Економічна безпека та кібербезпека взаємозалежні, оскільки кібератаки можуть спричиняти фінансові збитки, викрадення даних, зниження інвестиційної привабливості та порушення функціонування критичної інфраструктури. Надійна кібербезпека є важливою передумовою захисту економічних інтересів як окремих підприємств, так і держави загалом. Кіберзагрози можна класифікувати на декілька основних типів.

Шкідливе ПЗ. Шкідливе програмне забезпечення (або Malware) включає віруси, трояни, шпигунські програми і програми-вимагачі. Вони можуть завдати значної шкоди, починаючи від крадіжки даних і закінчуючи зупинкою функціонування інформаційних систем.

Фішинг. Це спроба отримати конфіденційну інформацію, таку як логіни і паролі, шляхом маскування під довірені джерела. Найчастіше використовується електронна пошта або підроблені веб-сайти.

Атаки типу «відмова в обслуговуванні» (DDoS). DDoS-атаки спрямовані на перевантаження мережевих ресурсів з метою їх відключення або порушення роботи. Ці атаки можуть призвести до значних втрат, особливо для онлайн-

сервісів. Цільові атаки (APT). Цільові постійні загрози (APT) – це складні і тривалі кібератаки, спрямовані на конкретні організації або особи [3].

Під час повномасштабної агресії розвиток галузі значною мірою залежить від фінансування за рахунок міжнародної технічної допомоги (наприклад, проекти USAID) або прямої підтримки світовими та національними компаніями. Зокрема, допомога США Україні в кібербезпеці протягом 2022-2024 років склала 82 млн доларів. Для порівняння: протягом 2016-2021 років це було 38 млн доларів. Тож за 9 років така допомога від США склала 120 млн доларів. Загалом протягом 2016-2024 років країнами-партнерами на розвиток інфраструктури кібербезпеки в Україні виділено 200 млн доларів (рис. 1).

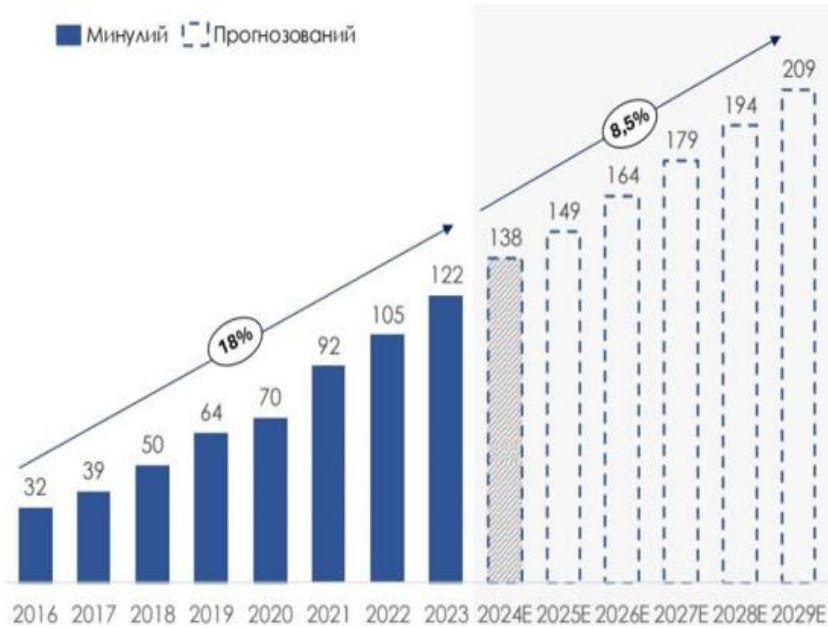


Рис. 1. Обсяг українського ринку кібербезпеки 2016-2029

Повномасштабна війна спричинила сплеск кібератак в Україні, підвищивши попит на автоматизовані рішення та інноваційні технології. Постійні кібератаки з боку російських хакерських угруповань частіше за все відбуваються на державні установи, ОПК, телекомунікації, фінансові установи та енергетику. У 2023 році зафіксовано 2544 кіберінцидентів, що на 16% більше від 2022 року. Водночас за даними CERT-UA у 2024 році опрацьовано 4315 кіберінцидентів, що майже на 70% більше від 2023 року [4].

Отже, у теперішніх умовах гарантування економічної безпеки неможливе без належного рівня кіберзахисту, оскільки інформаційні технології глибоко інтегровані в усі сфери суспільного життя та економіки. Кіберзагрози, зокрема шкідливе програмне забезпечення, фішинг, DDoS-атаки та цільові кібернапади, стають дедалі поширенішими й небезпечними, особливо в умовах воєнного стану. Україна, зіштовхуючись із масштабними кібератаками, змушена активно розвивати систему кібербезпеки за підтримки міжнародних партнерів. Надійний захист інформаційного простору є ключовою передумовою стабільного економічного розвитку, збереження національного суверенітету та безпеки громадян. Тому формування ефективної системи кіберзахисту має стати пріоритетом державної політики у сфері національної безпеки.

Література

1. Про основні засади забезпечення кібербезпеки України URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (20.04.2025)

2. Стеценко С. П. (2013). Економічна безпека: структура і сутність. URL: http://www.investplan.com.ua/pdf/24_2013/26.pdf

3. Як захиститися від кібератак. URL: https://itbiz.ua/statti-ta-obzori/yak-zahistitisya-vid-kiberatak/ (07.08.2024)

4. За останні 8 років ринок кібербезпеки в Україні зріс у 8 разів. URL: https://skilky-skilky.info/za-ostanni-8-rokiv-rynok-kiberbezpeky-v-ukraini-zris-u-8-raziv/ (13.01.2025)

5. Горбаченко С. (2020). Кібербезпека як складова економічної безпеки України URL: https://galicianvisnyk.tntu.edu.ua/pdf/66/903.pdf

6. Onyshchenko, S., Yanko, A., Hlushko, A., Maslii, O. (2023). Economic cybersecurity of business in Ukraine: strategic directions and implementation mechanism. Economic and cyber security. Kharkiv: PC TECHNOLOGY CENTER, 30–58. https://doi.org/10.15587/978-617-7319-98-5.ch2.

УДК 351.72

Фурманчук Оксана Сергіївна,
кандидат економічних наук, доцент
***Олексенко Ірина Іванівна**, студентка*
Національний університет «Полтавська політехніка імені Юрія Кондратюка»

РОЛЬ ФІНАНСОВОЇ ЗВІТНОСТІ У ЗАБЕЗПЕЧЕННІ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Фінансова звітність відіграє ключову роль у забезпеченні економічної безпеки підприємства, надаючи важливу інформацію для прийняття обґрунтованих управлінських рішень та своєчасного виявлення потенційних загроз. Її значення полягає в наступному:

1. Діагностика фінансового стану:

- аналіз ліквідності та платоспроможності. Це пов’язане з тим, що фінансова звітність, особливо Баланс та Звіт про рух грошових коштів, дозволяє оцінити здатність підприємства вчасно погашати свої поточні зобов'язання. Низькі показники ліквідності можуть свідчити про ризик неплатоспроможності