ЕКОНОМІКА **ECONOMICS**

Корчинська Олена. Кіберзлочинність як загроза економічній безпеці: світовий досвід та ситуація в Україні. *Економічний дискурс*. 2025. Випуск 1-2. С. 7-16.
DOI: https://doi.org/10.36742/2410-0919-2025-1-1

УДК 338.2: 004.056
JEL Classification F63:L86

Корчинська Олена
д.е.н., професор, професор кафедри маркетингу
Академія праці, соціальних відносин і туризму,
м. Київ, Україна
E-mail: helenk@meta.ua
ORCID: 0000-0003-2822-5634

КІБЕРЗЛОЧИННІСТЬ ЯК ЗАГРОЗА ЕКОНОМІЧНІЙ БЕЗПЕЦІ: СВІТОВИЙ ДОСВІД ТА СИТУАЦІЯ В УКРАЇНІ

Анотація

Вступ. *Світова практика свідчить про значне зростання кількості кіберінцидентів, зокрема атак на фінансові установи, підприємства критичної інфраструктури, державні інформаційні системи. За оцінками міжнародних організацій, щорічні економічні збитки від кіберзлочинності сягають сотень мільярдів доларів, створюючи серйозні виклики для формування стійкої економічної політики. Особливої актуальності ця проблема набуває для України, яка, з одного боку, активно впроваджує цифрові сервіси, а з іншого – стикається з обмеженими ресурсами у сфері кібербезпеки та зростанням рівня кібератак, пов'язаних із гібридними загрозами.*

Методи. *У статті використано комплексний підхід до аналізу проблеми кіберзлочинності як економічної загрози. Методологічну основу становлять загальнонаукові методи: аналіз, синтез, індукція, дедукція, а також спеціальні економічні методи – порівняльний аналіз, економічне моделювання, аналіз статистичних даних. Здійснено огляд міжнародних звітів з кібербезпеки, публікацій провідних дослідницьких установ, аналітичних центрів, а також нормативно-правових актів України та інших країн щодо протидії кіберзлочинності.*

Результати. *У результаті проведеного дослідження було встановлено, що кіберзлочинність є вагомим фактором дестабілізації економічної безпеки, особливо в умовах посиленої цифровізації економіки. Зокрема, визначено основні форми кіберзлочинності, які безпосередньо впливають на економіку: фінансові шахрайства, атаки на банки та компанії, викрадення конфіденційних даних, кібершантаж, порушення функціонування критичної інфраструктури. Проаналізовано світовий досвід стосовно даної проблеми. Вивчено поточний стан кібербезпеки в Україні, виявлено ключові проблеми: фрагментарність системи реагування, недостатність фінансування, нестача висококваліфікованих кадрів, а також зростання ризиків у зв'язку з гібридною війною. Запропоновано першочергові заходи для зменшення кіберекономічних загроз, серед яких – інституційне зміцнення сфери кібербезпеки, розвиток внутрішнього ринку кіберпослуг, стимулювання цифрової грамотності та формування системи економічного оцінювання збитків від кіберзлочинів.*

Перспективи. *У контексті динамічного розвитку цифрових технологій і змін у ландшафті кіберзагроз подальші дослідження можуть бути спрямовані на розробку методів кількісної оцінки економічних збитків від кіберзлочинності на рівні окремих галузей та підприємств, вивчення ефективності державної політики у сфері кібереконономічної безпеки, зокрема в умовах воєнного стану та визначення пріоритетних напрямів цифрової трансформації, що водночас підвищують економічну ефективність і знижують кіберризики.*

Ключові слова*: кіберзлочинність, економічна безпека, кіберзагрози, цифрова економіка, кібербезпека, фінансові втрати, національна безпека, інформаційні технології.*

Вступ.

У XXI столітті кіберзлочини стали серйозною загрозою для національних економік, міжнародної торгівлі, корпоративного сектора, державної безпеки тощо. Зростання рівня цифровізації та глобалізація бізнесу сприяють появі нових векторів кіберзагроз, які мають потенціал спричиняти значні фінансові, репутаційні та інші втрати.

Відповідно до Конвенції про кіберзлочинність, кіберзлочин – це суспільно небезпечне винне діяння, кримінальна відповідальність за яке передбачена законодавством, вчинене в кіберпросторі за допомогою електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, яке полягає в протиправному, несанкціонованому створенні, зберіганні, обробці, підробці, блокуванні, знищенні об'єктів інформаційної інфраструктури.

Таким чином, кіберзлочини охоплюють різноманітні сфери життя людей та будь-хто може стати їх жертвою.

Мета таких дій – розкрадання або руйнування інформації в інформаційних системах і мережах. В умовах війни кіберзлочини можуть здійснюватися з метою дестабілізації ситуації в країні, крадіжки необхідних (конфіденційних) даних, перешкоджання роботі державних інституцій, техніки, завдання іншої матеріальної шкоди.

Аналіз останніх досліджень та публікацій.

Проблематика кіберзлочинності та її впливу на економічну безпеку активно досліджується в останні роки як у вітчизняній, так і в зарубіжній науковій літературі. З огляду на стрімке зростання кількості та складності кібератак, дослідники все частіше розглядають кіберзлочинність не лише з технічної чи кримінологічної, а й з економічної точки зору.

На глобальному рівні помітними є публікації Світового економічного форуму [1], які відзначають, що економічні збитки від кіберзлочинів зростають експоненціально.

В українському науковому просторі питання кібербезпеки висвітлюються у працях Доценко Т. В., Кушнерьова О. С. [2], Золковер А. О., Кузьменко О. В., Койбічука В. В. [3].

Разом з тим, більшість досліджень зосереджена на технічних аспектах або загальній характеристиці загроз, тоді як економічні механізми впливу кіберзлочинності на фінансову стабільність, розвиток бізнесу та інвестиційний клімат залишаються недостатньо розробленими. Крім того, потребує уваги нинішня ситуація в України у зв'язку з війною та активною цифровізацією публічного сектору Це й зумовлює актуальність комплексного економічного аналізу кіберзлочинності як фактору національної безпеки.

Мета.

Мета – дослідити кіберзлочинність як чинник, що впливає на економічну безпеку держави, провести аналіз світового досвіду протидії даному явищу та дослідити поточну ситуацію в Україні. Обґрунтувати рекомендації щодо зміцнення економічної стійкості в умовах цифрових загроз.

Методологія дослідження.

У статті використано комплексний підхід до аналізу проблеми кіберзлочинності як економічної загрози. Методологічну основу становлять загальнонаукові методи: аналіз, синтез,

індукція, дедукція, а також спеціальні економічні методи – порівняльний аналіз, економічне моделювання, аналіз статистичних даних. Здійснено огляд міжнародних звітів з кібербезпеки, публікацій провідних дослідницьких установ, аналітичних центрів, а також нормативно-правових актів України та інших країн щодо протидії кіберзлочинності.

Результати.

Відповідно до Конвенції про кіберзлочинність, виділяють наступні види кіберзлочинів:

- правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ до систем; нелегальне перехоплення інформації; втручання у дані та системи; виготовлення, розповсюдження та збут шкідливого програмного забезпечення та спеціальних пристроїв);

-правопорушення, пов'язані з комп'ютерами (комп'ютерне підроблення та комп'ютерне шахрайство);

- правопорушення, пов'язані зі змістом (вироблення, володіння, розповсюдження або передача дитячої порнографії за допомогою комп'ютерних систем);

-правопорушення, пов'язані з порушенням авторських та суміжних прав.

Разом з цим, кіберзлочини, в залежності від наслідків та масштабу, можна поділити на дві категорії:

-кіберзлочини публічної дії, спрямовані на ураження комп'ютерних та інформаційно-телемунікаційних систем державних органів, міжнародних організацій, великих підприємств, державних реєстрів, об'єктів критичної інфраструктури та інших;

- кіберзлочини індивідувальної дії, спрямовані на заволодіння майном або інформацією певної особи, групи осіб або підприємства.

Найбільш популярними (розповсюдженими) останнім часом є кардинг, фішинг, вішинг, скімінг, шимінг, DDoS-атаки, ransomware та інші. Досить поширеним є також піратство – протиправне розповсюдження об'єктів інтелектуальної власності в Інтернеті. Згідно з даними Business Software Alliance 37% програмного забезпечення у світі є неліцензійним, що оцінюється у 46,3 млрд дол. США [4].

В останні роки ситуація з кіберзлочинність стає все більш напруженою. За даними Statista у 2022 році приблизно 40% користувачів інтернету по всьому світу повідомили, що стали жертвами кіберзлочинності, що свідчить про її масштабний вплив (рис. 1).

Найвищий показник був в Індії: близько 70% користувачів інтернету в Індії повідомили, що зазнали кіберзлочинів. Друге місце посіли США, де 49% респондентів зазначили, що стали жертвами інтернет-злочинів.

Така статистика відображає проблеми, пов’язані зі швидкою цифровізацією, збільшенням онлайн-активності та зростаючими вразливостями у сфері кібербезпеки, і це стосується як економічно розвинених країн світу, так і країн, що розвиваються.

Потенційно складніші технології, такі як штучний інтелект і хмарні технології, незважаючи на те, що ці інновації принесли багато переваг, створюють нові виклики як для безпеки бізнесу, індивідуальних користувачів, так і державних органів управління. Зараз майже вся інформація знаходиться в Інтернеті, і дані зберігаються переважно в електронному вигляді, тому кібернетика становить найбільший бізнес-ризик для організацій, запроваджуючи низку нових кіберризиків.

Так, середня світова вартість витоку даних у 2023 році становила 4,45 мільйона доларів США, що на 15% більше за останні три роки, і поки немає жодних ознак уповільнення, а навпаки. Відповідно до даних Національного центру кібербезпеки (NCSC) протягом 2023 року спостерігалось значне зростання кількості кіберінцидентів високого рівня. Одночасно із зростанням кількості кіберзлочинів, змінюється їх структура. Якщо у 2017 році приблизно 42% зареєстрованих кіберзлочинів були пов’язані з несплатою або недоставкою товарів і послуг, то у 2023 році більше половини припадає на фішинг та блокування доступу до даних [5].

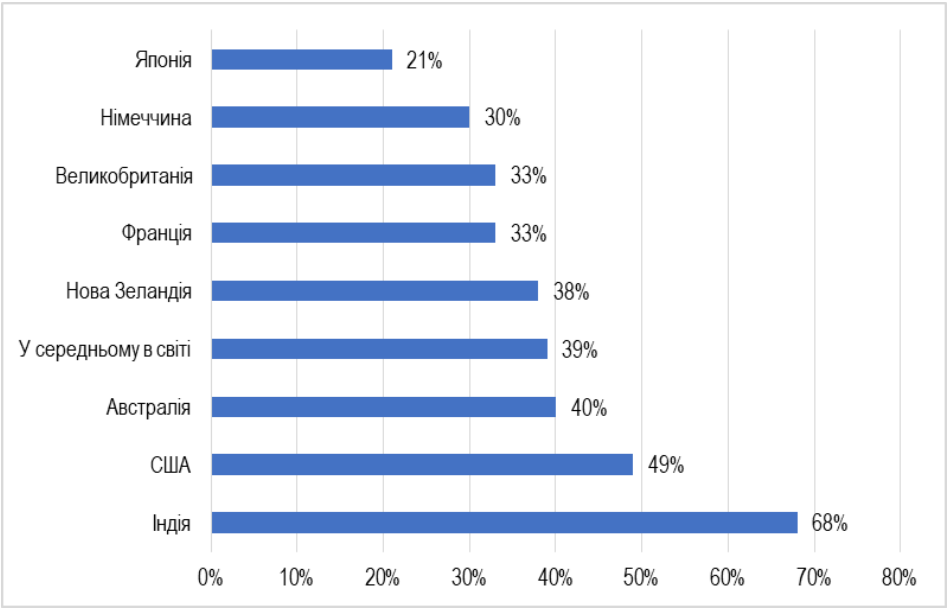

Рис. 1. Відсоток користувачів Інтернету, що стали жертвами кіберзлочинців, 2022 р.*
**Джерело: сформовано автором за даними [5].*

Спостерігається також тенденція до зростання ransomware атак. Так, у 2023 році 66% організацій у світі зафіксували кібератаки з метою шантажу та отримання викупу. Найвищий показник зафіксований в Сінгапурі, де 84% організацій постраждали від даного виду злочину. На другому місці – Південна Африканська Республіка (78%), далі йдуть Швейцарія (75%), Іспанія (75%) та Індія (73%) (рис. 2).

97% організацій змогли отримали свої дані назад, при цьому 46% організацій змушені були заплатити за таку можливість.

Середня сума викупу становила 1,5 млн. дол. США, при цьому зросла кількість організацій, які змушені були заплатити більше 1 млн. дол. США. Якщо у 2022 році частка таких організацій становила лише 11%, то у 2023 році вона досягнула 40%. На відновлення інформації 39% постраждалих витратили до 7 днів, 30% знадобилося майже місяць для відновлення.

Сектор освіти був найбільш схильний до атак програм-вимагачів у 2023 році: 80% (середня освіта) та 79% (вища освіта) повідомили про такі інциденти. Освіта традиційно стикається з нижчим рівнем фінансування та технологічного забезпечення, порівняно з багатьма іншими галузями, і дані свідчать про те, що зловмисники активно використовують ці слабкі місця.

Сектор IT, технологій та телекомунікацій зафіксував найнижчий рівень атак (50%), що свідчить про вищий рівень кіберготовності та кіберзахисту

Незалежно від рівня доходів, географічного розташування чи галузі, програми-вимагачі залишаються серйозною загрозою для організацій. Оскільки зловмисники продовжують вдосконалювати свої тактики, техніки і процедури, захисникам важко йти в ногу, що призводить до збільшення частоти кібератак та їх негативних наслідків.

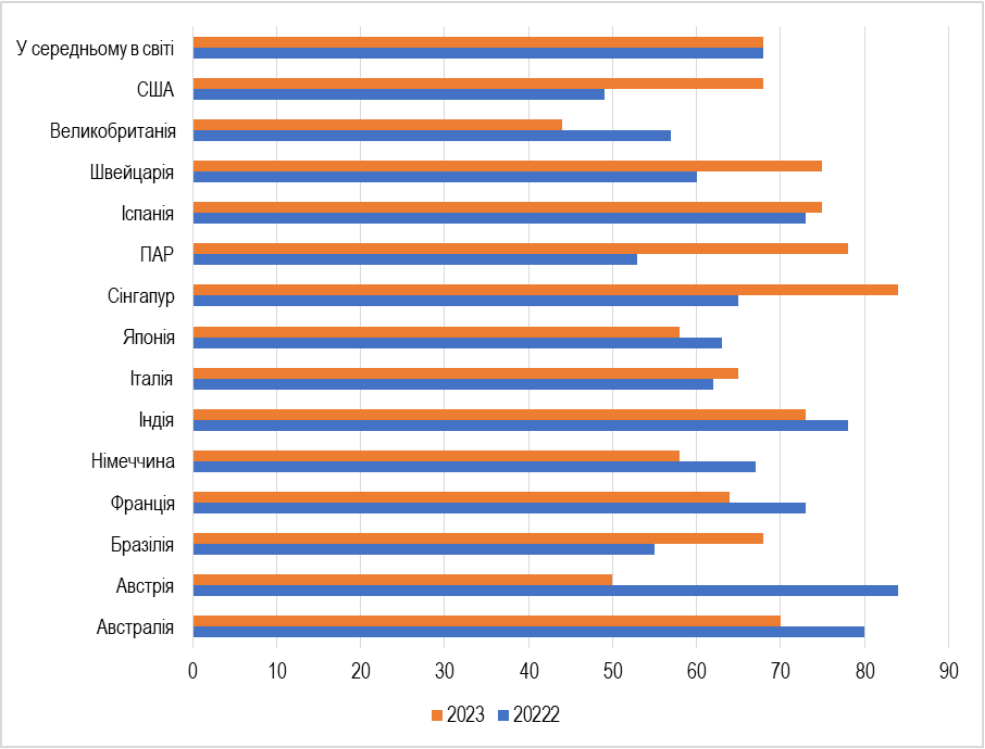

Рис. 2. Частка кібератак програмами-вимагачами (ransomware) у відсотках, 2022 і 2023 роки*
**Джерело: сформовано автором за даними [5].*

Однією з сучасних тенденцій також є зростання кількості атак на критичну інфраструктуру. Кібератаки на об'єкти критичної інфраструктури (енергетика, транспорт, медицина) стали більш поширеними. Хакери використовують такі атаки для вимагання грошей (ransomware) або дестабілізації. Особливо це відчувається в Україні з початку повномасштабного вторгнення росії. Так, за даними Служби безпеки України тільки у 2023 році було нейтралізовано майже чотири тисячі кібератак [6].

Нині злочинці по всьому світу активно використовують методи обману, які базуються на людській психології, так звану соціальну інженерію. Ця маніпулятивна тактика використовує людську психологію, щоб змусити людей розкривати конфіденційну інформацію або виконувати дії, які підривають безпеку. У той час як організації посилюють свої технічні засоби захисту, кіберзлочинці все більше звертаються до соціальної інженерії як основного вектора атаки, наприклад, як фішингу, щоб отримати доступ до конфіденційної інформації або змусити людей надати свої особисті дані. Згідно зі Звітом Verizon 2023 про порушення даних у 2023 році близько 74% кібератак на підприємства були спричинені помилками співробітників, пов'язаними саме із соціальною інженерією [7].

До сучасних тенденцій стосовно кіберзлочинів відносять і застосування хакерами штучного інтелекту, який допомагає розробляти складні віруси, аналізувати вразливості системи, підбирати паролі, генерувати фішинг-листи.

Країни з розвиненими економіками зазнають найбільших атак, оскільки вони мають складні цифрові системи, які широко застосовуються як бізнесовими структурами, так державними органами управління і пересічними громадянами.

Однією з таких країн, які стикаються з великою кількістю кібератак є США. У 2023 році інвестиційне шахрайство стало кіберзлочином, що завдало найбільших фінансових збитків громадянам США. Загальні втрати жертв у цій категорії перевищили 4,5 мільярда доларів США. На другому місці опинилося шахрайство через компрометацію ділової електронної пошти (BEC), яке призвело до втрат у розмірі близько 2,9 мільярда доларів США**.** Ще 924 мільйони доларів США було втрачено через шахрайство з технічною підтримкою (рис. 3).

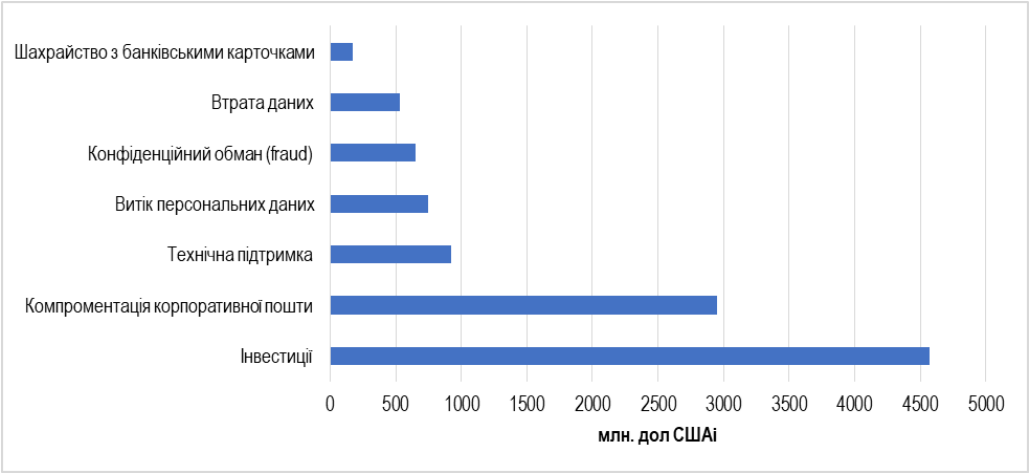

Рис. 3. Фінансові втрати через кіберзлочини в США у 2023 році, млн. дол. США*
**Джерело: сформовано автором за даними [5].*

Одним із викликів, з якими стикаються США, є постійний розвиток кіберзагроз, з якими традиційні заходи безпеки не в змозі впоратися. Крім того, взаємозв'язок цифрових систем і ланцюгів постачання запровадив нові вектори атак. Кіберзлочинці часто націлюються на сторонніх постачальників і партнерів, щоб дістатися до основної цілі.

Так було під час атаки на ланцюг поставок SolarWinds у 2020 році, коли зловмисники скомпрометували надійного постачальника програмного забезпечення, щоб отримати доступ до численних державних і корпоративних мереж. Такі епізоди підкреслюють необхідність більш цілісного підходу до кібербезпеки, який розглядає всю екосистему взаємопов'язаних систем.

Ризик кіберзлочинності та витоків даних також залишається високим і для компаній у Великій Британії (UK), особливо з огляду на розвиток штучного інтелекту останніми роками. На глобальному рівні британські компанії знаходяться в зоні найвищого ризику суттєвих кіберзагроз: близько 84% керівників з інформаційної безпеки (CISO) британських компаній підтверджують це. Однак, таку думку не завжди поділяють керівники компаній, адже менше половини з них стурбовані суттєвими кіберзагрозами в найближчому році [8].

Ця ситуація вкотре підтверджує розбіжності між поглядами CISO та членів рад директорів щодо кібербезпеки та оцінки майбутніх ризиків, хоча статистика підтверджує існування значної загрози з боку кіберзлочинців. Так, у 2022 році приблизно чотири з десяти британських компаній зафіксували кібернапад протягом року. Великі компанії виявилися більш уразливими до кіберзлочинності. У 2023 році, незважаючи на глобальну тенденцію до зростання атак програм-вимагачів, менше компаній у Великій Британії повідомили про такі атаки, порівняно з попереднім.

Станом на січень 2023 року, 11% компаній у Великій Британії стикалися з інцидентами витоків даних щотижня. Попри значну кількість кіберзлочинів, кількість витоків даних у Великій Британії зменшилася за останні два роки. Між першим кварталом 2020 року та третім кварталом

2023 року найбільше витоків даних було зафіксовано в першому кварталі 2021 року. У контексті щільності витоків даних, Великобританія перебуває в порівняно кращому стані, ніж інші країни світу [5].

Кіберзлочинність завдає значних збитків економікам усього світу. Станом на 2023 рік, щорічна вартість кіберзлочинності у Великій Британії оцінювалася у 320 мільярдів доларів США. Очікується, що ця цифра зросте до понад 1,82 трильйона доларів США до 2028 року. У 2022 році Великобританія, серед інших європейських ринків і США, другий рік поспіль зазнала найбільших втрат від кіберзлочинності – у середньому близько 4,21 мільйона доларів США за один витік даних [5].

Кіберзлочинство – це проблема не лише країн з розвиненою економікою. Наприклад, Індія також стикається з аналогічними викликами. За останні три роки кількість атак програмами – вимагачами (ransomware) зросла на 278%. Індія також зіткнулася зі сплеском атак на державні установи, кількість яких зросла на 460% за останні роки. Атаки програм-вимагачів поширюються в секторі кібербезпеки, виходячи за межі існуючих засобів захисту.

Найбільше постраждалим і вразливим є сектор малого та середнього бізнесу. Сучасні кібератаки використовують передові тактики, обходячи традиційне виявлення зловмисного програмного забезпечення та діючи в складних середовищах своїх цілей, спрямованих на викрадення даних, встановлювати програмне забезпечення-вимагач, шифрувати дані та викликати масові збої. Дослідження показало, що галузі, які розглядають виплату викупу, включають будівництво (74%), технології (51%) та енергетику (43%). [9]

Щодо України, то слід зазначити, що зараз країна знаходиться на передовій глобальної загрози кіберзлочинності. Ще до повномасштабного вторгнення росії як країни-агресорки Україна була однією з найбільш вразливих до кібератак країн, що зумовлено її геополітичним положенням, високою цифровізацією та конфліктами у кіберпросторі. З 2014 року Україна постійно стикається з кібератаками, які мають ознаки державного втручання. Одна з найвідоміших із них – це атака вірусу Petya/NotPetya у 2017 році, яка вразила тисячі систем уряду, банків та приватних компаній.

У період 2015–2016 рр. констатували напади на енергетичну інфраструктуру, зокрема зламування електромереж.

Під час повномасштабного вторгнення Росії в 2022 році фіксувався безпрецедентний рівень кібератак на державні установи, медіа, енергетику та інші сектори. Відзначається використання кібератак для інформаційної війни та дезінформації. Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, в 2024 році опрацювала 4315 кіберінцидентів [10].

Найчастіше зловмисники атакують місцеві органи влади, уряд та урядові організації, сектор безпеки та оборони, енергетичний сектор, комерційні організації, телекомунікації. Найпоширенішими типами інцидентів є розповсюдження шкідливого програмного забезпечення, фішинг, шкідливе підключення, компрометація облікового запису або системи. Метою зловмисників є викрадення чутливої інформації, а також знищення даних та інформаційних систем.

Водночас кіберзлочинці атакують і пересічних громадян. У 2022–2023 роках популярності набрали шахрайські схеми через Viber, Telegram та інші месенджери. Наприклад, «псевдо-волонтери» вимагали кошти на допомогу армії або постраждалим. Є випадки, коли через фальшиві мобільні додатки, пов'язані із війною (наприклад, додатки для перевірки тривог), встановлювалося програмне забезпечення для шпигунства або збору даних.

Наразі спостерігається стійка тенденція до зростання кібератак передусім на критично важливу інфраструктуру України. Ворог не полишає спроб дестабілізувати нашу країну і за допомогою кіберзброї. Це свідчить про те, що протистояння в кіберпросторі залишається однією з найгарячіших точок війни.

Є всі підстави стверджувати, що країна-агресорка продовжить застосовувати усі можливі методи для отримання інформації важливої для ворога. Не припинятимуться й деструктивні атаки

проти об'єктів критичної інфраструктури, зокрема енергетики.

Під час війни найціннішою для ворога є інформація про плани сил оборони України, дані підприємств оборонно-промислового комплексу, уряду та інших організацій, які здійснюють підтримку військових. Для досягнення цих цілей зловмисники зазвичай використовують масові розсилки шкідливого програмного забезпечення та фішингових листів. Такі типи кібератак залишаться наймасовішими.

Все вищезазначене вимагає застосування ряду заходів, спрямованих на зміцнення кібербезпеки. В Україні вже є позитивні зрушення у цьому напрямі. Так, у 2009 році був створений Департамент кіберполіції Національної поліції України, який представляє міжрегіональний територіальний орган Національної поліції України, і відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює, відповідно до законодавства, оперативно-розшукову діяльність, спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем.

У 2016 році було створено Національний координаційний центр кібербезпеки при РНБО. Серед основних завдань Центру: аналіз стану кібербезпеки; результатів проведення огляду національної системи кібербезпеки; стану готовності суб'єктів забезпечення кібербезпеки до виконання завдань з питань протидії кіберзагрозам; стану виконання вимог законодавства щодо кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також критичної інформаційної інфраструктури; даних про кіберінциденти стосовно державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо [11].

На державному рівні розроблено нову стратегію кібербезпеки України до 2025 року, яка визначає пріоритети, цілі та завдання забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Україна продовжує впроваджувати інновації у сфері кібербезпеки, але масштаб загроз вимагає постійної адаптації до нових викликів і більш активної участі громадян, бізнесових структур і державних органів управління.

Висновки і перспективи.

Кіберзлочинність є одним із ключових викликів економічній безпеці у XXI столітті. В умовах цифрової трансформації суспільства та економіки масштаби та складність кіберзлочинів невпинно зростають, завдаючи значних фінансових втрат як приватному сектору, так і державам у цілому. Досвід провідних країн світу демонструє, що ефективна протидія кіберзагрозам потребує комплексного підходу: правового регулювання, технічного забезпечення, міжсекторальної співпраці, активної участі бізнесу та інвестування в розвиток фахівців.

Аналіз ситуації в Україні свідчить про зростаючу вразливість до кіберзагроз на фоні війни, швидкої діджиталізації та обмежених ресурсів на кіберзахист. Незважаючи на наявність базових інституційних механізмів, система протидії кіберзлочинності вимагає подальшого вдосконалення, зокрема у сферах координації, реагування на інциденти, захисту критичної інфраструктури та підвищення фінансової грамотності бізнесу щодо цифрових ризиків.

Для посилення економічної стійкості України в умовах кіберзагроз доцільно:

- розширювати інвестиції у сферу кібербезпеки;
- розвивати партнерство між державою та приватним сектором;
- підвищувати рівень міжнародної співпраці;
- формувати культуру кібергігієни серед бізнесу та громадян.

Таким чином, кіберзлочинність є не лише кримінальним, а й глибоко економічним явищем,

яке потребує системного реагування як на національному, так і на глобальному рівні. Забезпечення економічної кібербезпеки має стати одним із пріоритетів державної політики України в найближчі роки.

Список використаних джерел

1. Світовий економічний форум. Global Cybersecurity Outlook 2024. URL: https://www.weforum.org/reports/global-cybersecurity-outlook-2024 (дата звернення: 06.02.2025).
2. Доценко Т. В., Кушнерьов О. С. Моделювання інтегрального індексу загрози національної економіки за допомогою метода Кернела. *Теорія та практика забезпечення розвитку кіберпростору України : монографія* / за ред. О. В. Кузьменко, Г. М. Яровенко. Київ : Інтерсервіс, 2020. С. 157–172.
3. Золковер А. О., Кузьменко О. В., Кушнерьов О. С., Койбічук В. В. Бібліометричний аналіз досліджень кіберзлочинності в умовах цифровізації фінансового сектору економіки держави. *Вісник Хмельницького національного університету*. 2019. №6 (Том 2). С. 253–259.
4. Business Software Alliance. Офіційний сайт. URL: https://www.bsa.org/ (дата звернення: 05.02.2025).
5. Statista. Офіційний сайт. URL: https://www.statista.com/statistics// (дата звернення: 06.02.2025).
6. 4000 кібератак на органи влади та критичну інфраструктуру – СБУ. URL: https://www.radiosvoboda.org/a/news-ataky-sbu-khakery/32621583.html (дата звернення: 05.02.2025).
7. 2023 Data Breach Investigations Report: frequency and cost of social engineering attacks skyrocket. URL: https://www.verizon.com/about/news/2023-data-breach-investigations-report (дата звернення: 04.02.2025).
8. UK Government Publishes Draft Code of Practice on Cybersecurity Governance. Hunton Andrews Kurth LLP. URL: https://www.huntonprivacyblog.com/2024/01/23/uk-government-publishes-draft-code-of-practice-on-cybersecurity-governance/ (дата звернення: 06.02.2025).
9. Sinha A. Safeguarding India's Digital Frontier: Unveiling Ransomware Challenges and Cybersecurity Strategies. Microsoft. URL: https://www.msn.com/en-in/money/news/safeguarding-indias-digital-frontier-unveiling-ransomware-challenges-and-cybersecurity-strategies (дата звернення: 06.02.2025).
10. Державна служба спеціального зв'язку та захисту інформації України. Офіційний сайт. URL: https://cip.gov.ua/ua/news/ (дата звернення: 06.02.2025).
11. Рада національної безпеки і оборони України. Офіційний сайт. URL: https://www.rnbo.gov.ua/ua/Diialnist/3303.html (дата звернення: 06.02.2025).

Статтю отримано: 24.02.2025 / Рецензування 09.04.2025 / Прийнято до друку: 30.06.2025

Olena Korchynska
Doctor of Economic Sciences, Professor, Professor
Department of Marketing
Academy of Labour, Social Relations and Tourism
Kyiv, Ukraine
E-mail: helenk@meta.ua
ORCID: 0000-0003-2822-5634

CYBERCRIME AS A THREAT TO ECONOMIC SECURITY: WORLD EXPERIENCE AND THE SITUATION IN UKRAINE

Abstract

Introduction. *Global practice demonstrates a significant increase in the number of cyber incidents, including attacks on financial institutions, critical infrastructure enterprises, and government information systems. According to estimates by international organizations, the annual economic losses from cybercrime amount to hundreds of billions of dollars, posing serious challenges to the development of sustainable economic policy. This issue is particularly relevant for Ukraine, which, on the one hand, is actively implementing digital services, and on the other hand, is facing limited resources in the field of cybersecurity and an increasing level of cyberattacks related to hybrid threats.*

Methods.*This article employs a comprehensive approach to analyzing the issue of cybercrime as an economic threat. The methodological framework is based on general scientific methods: analysis, synthesis, induction, deduction, as well as*

specialized economic methods – comparative analysis, economic modeling, and statistical data analysis. The study includes a review of international cybersecurity reports, publications by leading research institutions and think tanks, as well as legal and regulatory documents from Ukraine and other countries concerning cybercrime prevention.

Results. *The conducted research has shown that cybercrime is a significant destabilizing factor in economic security, especially in the context of intensified economic digitalization. In particular, the main forms of cybercrime directly impacting the economy have been identified: financial fraud, attacks on banks and companies, theft of confidential data, cyber extortion, and disruption of critical infrastructure operations. The global experience in countering cyber threats has been analyzed. The current state of cybersecurity in Ukraine has been examined, and key problems have been identified: fragmented response systems, insufficient funding, lack of highly qualified personnel, and rising risks due to hybrid warfare. Priority measures to mitigate cyber-economic threats are proposed, including institutional strengthening of the cybersecurity sector, development of the domestic cyber services market, promotion of digital literacy, and the formation of a system for economic assessment of losses from cybercrime.*

Prospects. *In the context of the dynamic development of digital technologies and changes in the cyber threat landscape, further research may focus on developing methods for quantitative assessment of economic losses from cybercrime at the level of specific industries and enterprises, analyzing the effectiveness of public policy in the field of cyber-economic security (particularly under martial law), and identifying priority areas of digital transformation that simultaneously enhance economic efficiency and reduce cyber risks.*

Keywords: *cybercrime, economic security, cyber threats, digital economy, cybersecurity, financial losses, national security, information technology.*

References

1. World Economic Forum. (2024). Global Cybersecurity Outlook 2024. Retrieved from https://www.weforum.org/reports/global-cybersecurity-outlook-2024

2. Dotsenko, T.V., & Kushneriov, O.S. (2020). Modeliuvannia intehralnoho indeksu zahrozy natsionalnoi ekonomiky za dopomohoiu metoda Kernela [Modeling the integral index of national economic threats using the Kernel method]. *Teoriia ta praktyka zabezpechennia rozvytku kiberprostoru Ukrainy : monohrafiia.* Kuzmenko, O. V. & Yarovenko, H. M. (Eds.). Kyiv: Intersystem, 157–172.

3. Zolkover, A.O., Kuzmenko, O.V., Kushneriov, O.S., & Koibichuk, V.V. (2019). Bibliometrychnyi analiz doslidzhen kiberzlochynnosti v umovakh tsyfrovizatsii finansovoho sektoru ekonomiky derzhavy [Bibliometric analysis of cybercrime research in the context of digitalization of the national financial sector]. *Visnyk of Khmelnytskyi National University* [Bulletin of Khmelnytskyi National University], *6 (2)*, 253–259. [in Ukr.].

4. Business Software Alliance. (n.d.). Official website. Retrieved from https://www.bsa.org/

5. Statista. (n.d.). Official statistics portal. Retrieved from https://www.statista.com/statistics//

6. 4000 kiberatak na orhany vlady ta krytychnu infrastrukturu – SBU. Retrieved from https://www.radiosvoboda.org/a/news-ataky-sbu-khakery/32621583.html/

7. 2023 Data Breach Investigations Report: Frequency and cost of social engineering attacks skyrocket. Retrieved from https://www.verizon.com/about/news/2023-data-breach-investigations-report.

8. Hunton Andrews Kurth LLP. UK Government publishes draft code of practice on cybersecurity governance. Retrieved from https://www.huntonprivacyblog.com/2024/01/23/uk-government-publishes-draft-code-of-practice-on-cybersecurity-governance/

9. Sinha, A. (2024). Safeguarding India's digital frontier: Unveiling ransomware challenges and cybersecurity strategies. Microsoft. Retrieved from https://www.msn.com/en-in/money/news/safeguarding-indias-digital-frontier-unveiling-ransomware-challenges-and-cybersecurity-strategies.

10. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. Ofitsiinyi sait.. Retrieved from https://cip.gov.ua/ua/news/

11. Rada natsionalnoi bezpeky i oborony Ukrainy. Ofitsiinyi sait. Retrieved from https://www.rnbo.gov.ua/ua/Diialnist/3303.html.

Received: 02.24.2025 / Review 04.09.2025 / Accepted 06.30.2025