

Яковишин В.,
здобувач першого(бакалаврського) рівня вищої освіти,
Кудельський В.Е.,
к.е.н., доцент,
Хмельницький університет управління та права імені Леоніда Юзькова

РОЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ У ПІДТРИМЦІ ДОВІРИ ДО ЦИФРОВОЇ ЕКОНОМІКИ

У сучасному глобалізованому світі цифрова економіка стрімко трансформує традиційні бізнес-моделі, забезпечуючи нові можливості для зростання, інновацій і доступу до ринків. Водночас фундаментом її ефективного функціонування є довіра користувачів, інвесторів і державних інституцій, яка неможлива без високого рівня інформаційної безпеки. Інформаційна безпека виступає критичним чинником забезпечення конфіденційності, цілісності та доступності даних, що лежать в основі цифрових транзакцій, електронної комерції, фінансових технологій і державних цифрових сервісів.

Цифрова економіка України, як частина глобального процесу цифровізації, інтенсивно розвивається в умовах військової агресії, нестабільного безпекового середовища та високих ризиків кіберзагроз. Проте саме довіра до цифрових платформ, сервісів і державних е-послуг стає критично важливою умовою подальшого зростання цифрової економіки. Інформаційна безпека в цьому контексті виконує ключову роль – вона не лише забезпечує захист даних, але й формує впевненість громадян, бізнесу та інституцій у стабільності цифрового середовища.

Згідно з даними Офісу Президента та Міністерства цифрової трансформації України, у 2023 році понад 19 мільйонів громадян скористалися цифровими послугами через платформу «Дія». Це стало можливим завдяки активному розвитку кіберзахисту, запровадженню національної стратегії кібербезпеки та підвищенню стійкості державних інформаційних систем. Однак паралельно з ростом цифрових сервісів в Україні фіксується збільшення кількості кібератак – за даними Держспецв'язку, у 2023 році кількість виявлених кіберінцидентів зросла на 38% порівняно з попереднім роком.

Таблиця 1 - Динаміка кібератак на державні та комерційні інформаційні системи в Україні (2021–2023)

Рік	Кількість інцидентів	Основні цілі атак
2021	24 500	Банки, освітні платформи
2022	35 900	Дія, державні реєстри
2023	49 600	Електронна пошта, е-урядові сервіси, медичні системи

Джерело: Складено на основі [1]

Державна підтримка також відіграє важливу роль. Національний координаційний центр з кібербезпеки України надає рекомендації щодо захисту критичної інфраструктури. Участь у державних ініціативах, таких як навчальні семінари та обмін інформацією про загрози, сприяє підвищенню стійкості бізнесу. Ефективне управління ризиками передбачає наявність чітких планів дій у разі інцидентів. Понад 80% успішних компаній мають розроблені протоколи реагування, які включають залучення спеціалізованих команд, резервування даних та співпрацю з правоохоронними органами. Наприклад, компанії, що впровадили такі протоколи, скоротили час відновлення після атак з 72 до 24 годин.

Сучасні технології стають важливим інструментом у боротьбі з кіберзагрозами. Використання багаторівневих систем захисту, зокрема SIEM (Security Information and Event Management), дозволяє підприємствам оперативно виявляти та реагувати на інциденти. Понад 40% компаній, які впровадили SIEM-системи, відзначили зниження кількості успішних атак на 30% протягом першого року використання. Штучний інтелект також активно застосовується для аналізу аномалій у мережевій активності. Наприклад, алгоритми машинного навчання дозволяють скоротити час виявлення загроз з декількох годин до кількох хвилин, що особливо важливо для великих підприємств, де щодня генерується значний обсяг даних. [3]

Поширення цифрових технологій, зокрема у фінансовому секторі, освіті, охороні здоров'я та держуправлінні, потребує системного підходу до інформаційної безпеки. Згідно з дослідженням, опублікованим у фаховому журналі «Public Management» (2023), основними бар'єрами до формування

довіри в цифровому середовищі є: низький рівень цифрової грамотності населення, слабка культура кібергігієни, обмежене фінансування безпекових рішень у малому бізнесі, а також недостатня прозорість у поводженні з персональними даними.

У цьому контексті інформаційна безпека стає передумовою економічної стабільності. Порушення конфіденційності даних може призвести до фінансових втрат, падіння репутації компаній, зменшення участі споживачів у цифрових продуктах і послугах, а також недовіри до державних інститутів.

Таблиця 2 - Вплив кіберінцидентів на довіру користувачів до цифрових сервісів в Україні

Частота зіткнення з кіберзагрозами	Довіра до цифрових послуг (%)	Готовність користуватись знову (%)
Часто (1+ разів на місяць)	41	33
Іноді (1 раз на пів року)	66	58
Не стикались	83	77

Джерело: складено на основі [2]

Таким чином, інформаційна безпека є не лише технічним завданням, а й стратегічною передумовою сталого цифрового розвитку. Без належного захисту даних, цифрова економіка втрачає головне — довіру, яка є основою для інновацій, електронного урядування та глобальної інтеграції. З огляду на це, необхідно зміцнювати кіберстійкість на всіх рівнях: від персонального до національного, що має бути інтегрованим у державну політику, бізнес-стратегії та освітні програми.

Список використаних джерел

1. Державна служба спеціального зв'язку та захисту інформації України.
<https://www.cip.gov.ua/ua>
2. Динаміка довіри соціальним інституціям у 2021-2024 роках.
<https://www.kiis.com.ua/?lang=ukr&cat=reports&id=1467&page=3>
3. Забезпечення інформаційної безпеки бізнесу України в умовах сучасних загроз. <https://repository.sspu.edu.ua/server/api/core/bitstreams/9175f480-2f6f-428a-80a8-166acdc0ea03/content>