О. В. ОРЛИК
канд. екон. наук, доц.,
доцент кафедри економічної кібернетики та інформаційних технологій,
Одеський національний економічний університет

К. О. ПЛУКЧІ
здобувачка вищої освіти,
Одеський національний економічний університет

КІБЕРБЕЗПЕКА В УМОВАХ ЗРОСТАННЯ ЦИФРОВИХ ЗАГРОЗ

У сучасному світі стрімкий розвиток цифрових технологій докорінно змінює всі аспекти нашого життя — від спілкування та бізнесу до державного управління і захисту даних. Разом із цими можливостями зростає і загроза кіберзлочинності, яка передбачає незаконні дії у цифровому просторі, серед яких: хакерські атаки, фішинг, фінансові махінації, крадіжка особистих даних та навіть кібершпигунство. Кібербезпека стала однією з ключових проблем, що стоїть перед урядом країни, бізнесом і громадянами, адже цифрові ризики та загрози можуть мати глобальні наслідки для економіки, національної безпеки та соціальної стабільності.

Актуальність питання забезпечення кібербезпеки полягає у тому, що з кожним роком зростає кількість кібератак, які стають більш складними і масштабними. Напади на критичну інфраструктуру, порушення конфіденційності даних та витоки інформації створюють серйозні загрози для безпеки держави, бізнесу та громадян. У цих умовах розробка надійних систем кіберзахисту, удосконалення законодавства та формування культури безпеки серед користувачів є необхідними кроками для збереження стабільності у цифровому просторі.

Сучасна цифрова епоха, що характеризується стрімким розвитком технологій, ставить перед людством важливе завдання забезпечення кібербезпеки. Збільшення обсягів цифрової інформації та широке впровадження інноваційних цифрових технологій зумовлюють ризики та загрози несанкціонованого доступу до даних і їх неправомірного використання. Цифрова трансформація не лише створює нові можливості для розвитку суспільства, але й створює додаткові вразливі точки у сфері захисту персональних даних, критичних інфраструктур, корпоративних систем і мереж.

Особливу увагу варто приділити викликам, пов'язаним із поширенням технологій "Інтернету речей" (IoT). Величезна кількість взаємопов'язаних пристроїв забезпечує високий рівень комфорту та автоматизації, але водночас відкриває нові шляхи для потенційних атак на ці системи. Несанкціоноване втручання в роботу таких пристроїв може мати негативний вплив не лише на окремі організації, але й на суспільство в цілому [1].

За даними досліджень Массачусетського технологічного інституту, у 2023 році кількість витоків даних зросла на 20 % порівняно з попереднім роком, а кібератаки програм-вимагачів (ransomware) збільшилися майже на 70 %. Серед основних причин цих загроз: неправильна конфігурація хмарних середовищ, поява нових і більш шкідливих програм-вимагачів, а також активізація використання систем постачальників, вразливості в яких можуть використовувати зловмисники, щоб отримати доступ до клієнтів, які використовують ці послуги. Так, близько 80 % витоків даних у 2023 році були пов'язані із хмарними сховищами, що свідчить про необхідність більш ретельної уваги до безпеки цих технологій [2].

В умовах зростання цифрових загроз потрібно: обмежувати кількість особистих даних, що зберігаються у зручному для читання форматі: використовувати програмні рішення, які впроваджують наскрізне шифрування, щоб зменшити кількість збережених вразливих даних, які становлять ризик для людей; навчати співробітників щодо обов'язків у сфері кібербезпеки.

Зростання негативних фінансових наслідків, спричинених кіберзагрозами, викликає необхідність підвищення рівня інформаційної безпеки в процесі розвитку цифрової інфраструктури. Наразі існує кілька глобальних індексів, які дають можливість оцінити кіберпотужність країни та її здатність протистояти кіберзагрозам. Зокрема, оцінити ефективність регуляторних заходів та засобів для досягнення стратегічних цілей у сфері кібербезпеки [3, с. 16].

Наприкінці слід зазначити, що зростання обсягу цифрових даних, впровадження "Інтернету речей" і розвиток хмарних технологій значно збільшу-

ють вразливість критичної інфраструктури до кібератак. Успішне вирішення цієї проблеми потребує активної взаємодії між урядом, бізнесом та громадянським суспільством, удосконалення нормативно-правової бази, розвитку освітніх ініціатив і запровадження інноваційних технологій для захисту цифрових даних. Лише системний підхід до забезпечення кібербезпеки дозволить мінімізувати ризики й загрози та зберегти стабільність у цифровому просторі.

Джерела

1. *Капітон А. М.* Кібербезпека в епоху цифрової трансформації. https://surl.li/cuoxii (дата звернення: 27.01.2025).
2. *Stackpole B.* MIT report details new cybersecurity risks. URL: https://surl.li/tonwov (дата звернення: 27.01.2025).
3. *Онищенко С. В., Глушко А. Д.* Аналітичний вимір кібербезпеки України в умовах зростання викликів та загроз. *Економіка і регіон.* 2022. № 1 (84). С. 13–20. DOI: https://doi.org/10.26906/EiR.2022.1(84).2540.