

МАТЕРІАЛИ

II ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ МОЛОДИХ ВЧЕНИХ

«Математичні методи та цифрові
технології в економіці»

17 КВІТНЯ 2025 РОКУ
М. ІРПІНЬ

МАТЕМАТИЧНІ МЕТОДИ ТА ЦИФРОВІ ТЕХНОЛОГІЇ В ЕКОНОМІЦІ

Збірник тез

II Всеукраїнської науково-практичної конференції молодих вчених

17 квітня 2025 р.

ЕЛЕКТРОННЕ ВИДАННЯ

Ірпінь
2025

УДК 519.87(06)
ББК 65в631я431
М 34

Рекомендовано до друку
Вченою радою Державного податкового університету
(протокол № 15 від 29 травня 2023 р.)

Математичні методи та цифрові технології в економіці
М 34 [Електронне видання] : збірник тез II Всеукраїнської науково-практичної конференції молодих вчених, м. Ірпінь, 17 квітня 2025 р. – Ірпінь : Державний податковий університет, 2025. – 278 с. – PDF-формат ; мережеве видання ; інституційний репозитарій.
ISBN 978-966-337-772-8

Збірник містить тези II Всеукраїнської науково-практичної конференції молодих вчених «Математичні методи та цифрові технології в економіці», що відбулася 17 квітня 2025 р. в Державному податковому університеті.

У межах конференції було висвітлено питання популяризації передових математичних і цифрових підходів до аналізу економічних процесів, розвитку наукового потенціалу молодих учених та їхньої активної участі в дослідженнях у сфері економіки, фінансів і цифрових технологій, інтеграції математичних методів у практику економічного прогнозування, моделювання й управління ризиками. Особливу увагу приділено перспективам застосування цифрових технологій, штучного інтелекту та великих даних у фінансово-економічному секторі, а також обміну досвідом між молодими дослідниками, викладачами й представниками бізнесу щодо впровадження інноваційних математичних та інформаційних технологій в економічну діяльність. Конференція сприяла формуванню нових наукових колаборацій, розширенню контактів на національному й міжнародному рівнях і стала унікальним майданчиком для інтеграції фундаментальних і прикладних досліджень у практичну діяльність, що має ключове значення для розвитку цифрової економіки України.

II Всеукраїнська науково-практична конференція молодих вчених «Математичні методи та цифрові технології в економіці» стала важливою подією для наукової спільноти, об'єднавши дослідників, викладачів і представників бізнесу з метою обговорення сучасних тенденцій у розвитку економіки, фінансів і цифрових технологій. Учасники мали можливість представити результати власних наукових пошуків, поділитися практичним досвідом та отримати конструктивний зворотний зв'язок від колег і провідних фахівців.

Видання призначене для науковців, молодих учених, аспірантів, студентів.

Матеріали подано в авторській редакції.
Відповідальність за зміст матеріалів, їх відповідність вимогам чинного правопису та достовірність фактів і статистичних даних несуть автори.

УДК 519.87(06)
ББК 65в631я431

ISBN 978-966-337-772-8

© Державний податковий університет, 2025

Бойко Микита, Мельник Людмила РОЗВИТОК ГРОМАД В УКРАЇНІ ЯК ЕЛЕМЕНТ СМАРТ-СПЕЦІАЛІЗАЦІЇ.....	169
Митусь Анастасія, Лаговський Володимир АВТОМАТИЗАЦІЯ БІЗНЕС-ПРОЦЕСІВ У МАЛОМУ ТА СЕРЕДНЬОМУ БІЗНЕСІ ЗА ДОПОМОГОЮ ІТ-РІШЕНЬ.....	172
Мірошніченко Інга РОЗВИТОК МЕТАВСЕСВІТУ: ПОТЕНЦІАЛ ЦИФРОВИХ ТЕХНОЛОГІЙ У МАКРОЕКОНОМІЦІ.....	175
Мітла Марія, Грищенко Світлана РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ ТА АВТОМАТИЗАЦІЇ.....	177
Морозов Олександр, Омельчук Антон ОПТИМІЗАЦІЯ БІЗНЕС-ПРОЦЕСІВ ПРОГРАМНИХ ЗАСТОСУНКІВ У ФІНАНСОВІЙ ГРАМОТНОСТІ ЗА ДОПОМОГОЮ ІНСТРУМЕНТУ UNITY.....	180
Муравський Олесь, Дудник Олексій ЦИФРОВІ ТЕХНОЛОГІЇ ТА МАТЕМАТИЧНІ МЕТОДИ В УПРАВЛІННІ СПОРТИВНИМИ ЗАХОДАМИ.....	184
Мусійчук Дмитро, Лаговський Володимир ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ФІНАНСОВОМУ ПРОГНОЗУВАННІ.....	188
Ніколаєнко Дмитро, Густера Олег ВИКОРИСТАННЯ СУЧАСНИХ МЕТОДІВ MACHINE LEARNING ДЛЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ОНЛАЙН-РЕСУРСІВ.....	190
Отвага Микола, Пузирьова Поліна КІБЕРБЕЗПЕКА ПІДПРИЄМСТВ ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ	193
Пилипенко Денис, Омельчук Антон СТВОРЕННЯ НАВЧАЛЬНОГО ВЕБЗАСТОСУНКУ З МОЖЛИВІСТЮ МОДЕЛЮВАННЯ КРИПТОВАЛЮТНОЇ БІРЖІ	197

Микола Отвага,
здобувач другого (магістерського)
рівня вищої освіти,
кафедра смарт-економіки
email: otvagakolya@gmail.com

Науковий керівник:
Поліна Пузирьова,
д-р екон. наук, професор,
кафедра смарт-економіки,
Київський національний університет
технологій та дизайну
email: puzyrova@ukr.net

КІБЕРБЕЗПЕКА ПІДПРИЄМСТВ ЯК ОСНОВА ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВІЗАЦІЇ

У сучасну епоху цифровізації, коли інформаційні технології глибоко інтегровані у всі сфери економіки, питання кібербезпеки підприємств набуває особливого значення. Цифрові платформи, хмарні сервіси, онлайн-платежі, автоматизовані системи управління – усе це створює нові можливості для розвитку бізнесу, але водночас підвищує ризики, пов'язані з витоком конфіденційної інформації, фінансовими шахрайствами та кібератаками [1–2]. У цьому контексті кібербезпека підприємства виступає не лише інструментом захисту внутрішніх активів, але й ключовим чинником забезпечення міжнародної економічної безпеки, особливо в умовах глобальної цифрової взаємозалежності.

Кібербезпека підприємства – це комплекс організаційних, технічних, програмних та правових заходів, спрямованих на захист інформаційних ресурсів, бізнес-процесів, фінансових і персональних даних від несанкціонованого доступу, кіберзлочинності, атак, зловмисного програмного забезпечення та інших загроз у кіберпросторі. Основними структурними елементами кібербезпеки підприємств є: інформаційна безпека – захист комерційної, персональної та технічної інформації; технічна безпека – застосування апаратних засобів контролю доступу, мережевих фільтрів, серверного захисту; програмна безпека – використання антивірусів, брандмауерів, систем виявлення загроз; організаційна безпека – регламентація доступу, інструкції для персоналу, політика безпеки; правова безпека – дотримання вимог законодавства (GDPR, ISO/IEC 27001 тощо); кадрова безпека – навчання працівників правилам цифрової гігієни та поведінки в мережі [3–4].

Ключові принципи, функції та задачі кібербезпеки наведено у табл. 1.

Таблиця 1 – Принципи, функції та задачі кібербезпеки підприємств
в умовах цифровізації [1–3]

Принципи	Функції	Основні задачі
Конфіденційність	Виявлення слабких місць в ІТ-системах	Забезпечення захисту критичних даних і комерційної таємниці
Цілісність	Моніторинг кіберзагроз у реальному часі	Підвищення цифрової грамотності працівників
Доступність	Запобігання несанкціонованому доступу	Створення стійкої та гнучкої ІТ-інфраструктури
Прозорість	Реагування на інциденти безпеки	Упровадження систем управління інформаційною безпекою
Безперервність	Відновлення роботи після атак (disaster recovery)	Впровадження систем резервного копіювання та планів відновлення
Адаптивність	Аналіз та аудит ІТ-інфраструктури	Формування культури безпеки в межах корпоративного середовища

Досягнення високого рівня кіберзахисту вимагає системного, багатоетапного підходу, який охоплює всі ключові сфери діяльності підприємства. Алгоритм, який дозволяє підприємству ефективно будувати й підтримувати кібербезпеку складається з таких етапів [1–4]:

Етап 1. Аудит ІТ-інфраструктури. Першим кроком є всебічний аудит інформаційної інфраструктури підприємства, що включає інвентаризацію всіх апаратних і програмних засобів, мережевих елементів, баз даних, серверів, облікових записів та інших компонентів.

Етап 2. Оцінка ризиків. Після аудиту здійснюється ідентифікація потенційних кіберзагроз, таких як фішинг, віруси, DDoS-атаки, витік даних, шкідливе програмне забезпечення тощо. На цьому етапі також аналізується ймовірність виникнення кожної загрози та масштаби можливих збитків, що дозволяє встановити пріоритети у сфері захисту, розподілити ресурси та визначити найбільш критичні напрями для реагування.

Етап 3. Формування політики безпеки. Після оцінки загроз підприємство розробляє внутрішню політику кібербезпеки, яка визначає рівні доступу, алгоритми реагування на інциденти, правила створення паролів, порядок використання особистих пристроїв, шифрування даних, резервне копіювання та інші аспекти.

Етап 4. Впровадження технічних рішень. Впровадження конкретних технічних засобів захисту передбачає: антивірусні програми для виявлення й нейтралізації шкідливого ПЗ; брандмауери (Firewall) для фільтрації трафіку; VPN для безпечного з'єднання віддалених користувачів; системи контролю доступу до ресурсів; SIEM-системи, які забезпечують централізований моніторинг та аналіз подій безпеки; резервне копіювання та хмарні сервіси для забезпечення відновлення даних у разі втрати або пошкодження.

Етап 5. Навчання персоналу. Людський чинник – одна з причин витоків і порушень безпеки, тому навчання працівників є стратегічно важливим етапом, що включає: проведення регулярних тренінгів з цифрової гігієни; ознайомлення зі сценаріями шахрайства; імітації кібератак для перевірки готовності персоналу; внутрішні тести знань з інформаційної безпеки.

Етап 6. Моніторинг і контроль. Після впровадження засобів захисту важливо забезпечити постійне відстеження подій у мережі підприємства: аналіз логів (журналів подій); виявлення аномального трафіку; попередження несанкціонованих спроб доступу; визначення слабких місць у реальному часі.

Етап 7. Реагування на інциденти. Кожне підприємство повинне мати чітко прописаний план реагування на інциденти. У разі виявлення кібератаки алгоритм дій може включати: ізоляцію ураженої частини мережі; сповіщення відповідальних осіб; активацію систем відновлення; документування події та її наслідків; повідомлення партнерів або клієнтів (у разі витоку).

Етап 8. Аналіз та вдосконалення. На цьому етапі відбувається постійний перегляд ефективності заходів кібербезпеки. На основі аналізу інцидентів, звітів моніторингу та зовнішніх змін підприємство повинне оновлювати свою політику, модернізувати технічні засоби та адаптувати стратегії. В цьому контексті кібербезпека – це не разова дія, а безперервний процес, який потребує гнучкості та готовності до змін.

Отже, можемо підсумувати, що ефективна кібербезпека – це результат системного, багаторівневого підходу, в якому важливе місце займає як технічне оснащення, так і людський чинник. У глобалізованій цифровій економіці кібербезпека окремих підприємств безпосередньо впливає на стабільність міжнародних економічних відносин. Атаки на банки, енергетичні компанії, логістичні платформи або системи електронних торгів можуть мати ланцюговий ефект і викликати збитки на міждержавному рівні, а саме тому кібербезпека стає не лише внутрішнім завданням бізнесу, а й елементом геополітичної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дубина М., Заєць О. Забезпечення кібербезпеки підприємств електронної комерції в умовах становлення цифрової економіки. *Scientific Bulletin of Polissia*. 2024. № 1 (28). С. 208–223. URL : [https://doi.org/10.25140/2410-9576-2024-1\(28\)-208-223](https://doi.org/10.25140/2410-9576-2024-1(28)-208-223)
2. Пузирьова П. В. Механізм забезпечення економічної безпеки у сфері сталого розвитку фінансової системи держави в умовах цифрової економіки та глобалізаційних змін. *Актуальні проблеми економіки*. 2025. № 1 (283). С. 189–204. URL : <https://doi.org/10.32752/1993-6788-2025-1-283-189-204>
3. Bondar-Pidhurska O. V., Khomenko I. I. Scientific and Methodological Principles of Assessing the Efficiency of the Information Security Process Management of Small and Medium-Sized Businesses: Cybersecurity and Intellectual Property. *The Problems Of Economy*. 2022. Vol. 2, no. 52. P. 108–116. URL : <https://doi.org/10.32983/2222-0712-2022-2-108-116>

4. Kukshyn D. V. Methods for assessing the state of protection of enterprises from cybersecurity threats. *Modern Information Security*. 2021. Vol. 47, no. 3. URL : <https://doi.org/10.31673/2409-7292.2021.035565>

Наукове електронне мережеве видання

Математичні методи та цифрові технології в економіці

Збірник тез

II Всеукраїнської науково-практичної конференції молодих вчених

17 квітня 2025 р.

ЕЛЕКТРОННЕ ВИДАННЯ

Укладач

*Ярова О. А.,
Скасків Л. В.,
Омельчук А. А.*

Відповідальний за випуск

Добрянська Н. Б.

Форматування та
комп'ютерна верстка

Завальницька Д. П.

Друк. арк. 16.1
Замовлення № 1152

*Підготовлено науково-організаційним відділом
Державного податкового університету
08205, вул. Університетська, 31, м. Ірпінь, Київська область, Україна*

*Свідоцтво про внесення суб'єкта видавничої справи
до державного реєстру видавців, виготовників
і розповсюджувачів видавничої продукції
Серія ДК № 7669 від 20.09.2022*