МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
МАРІУПОЛЬСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

АКТУАЛЬНІ ПРОБЛЕМИ НАУКИ ТА ОСВІТИ

Збірник матеріалів

XXVIII підсумкової науково-практичної конференції викладачів

24 лютого 2026

Київ 2026

УДК 061.3(063)

АКТУАЛЬНІ ПРОБЛЕМИ НАУКИ ТА ОСВІТИ: Збірник матеріалів XXVIII підсумкової науково-практичної конференції викладачів МДУ / За заг. ред. Т.В. МАРЕНИ, Київ: МДУ, 2026. с. 350

Рекомендовано до друку та поширення через мережу Інтернет вченою радою Маріупольського державного університету (протокол № 9 від 25 лютого 2026 року)

Збірник містить матеріали XXVIII підсумкової науково-практичної конференції викладачів МДУ, яка відбулася 24 лютого 2026 року в Маріупольському державному університеті.

У матеріалах висвітлені актуальні проблеми розвитку міжнародних відносин та зовнішньої політики, філософії та соціології, історії, економіки та менеджменту, права, екології, кібербезпеки, документознавства, культурології, журналістики, філології, літературознавства, методики викладання, педагогіки та психології.

Видання адресоване науковцям, викладачам, аспірантам та здобувачам вищої освіти, а також усім, хто цікавиться сучасними проблемами науки та освіти.

Редакція не несе відповідальності за авторський стиль тез, опублікованих у збірнику.

Література

1. Boston Consulting Group. GenAI increases productivity & expands capabilities. 2024. URL: https://www.bcg.com/publications/2024/gen-ai-increases-productivity-and-expands-capabilities (дата звернення: 15.01.2026)

2. Challapally, A., Pease, C., Raskar, R., & Chari, P. The GenAI Divide: State of AI in Business 2025 (v0.1). 2025. MIT NANDA. URL: https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf (дата звернення: 15.01.2026)

3. Dell'Acqua, F., McFowland III, E., Mollick, E. R., Lifshitz-Assaf, H., Kellogg, K., Rajendran, S., Krayer, L., Candelon, F., & Lakhani, K. R. Navigating the jagged technological frontier: Field experimental evidence of the effects of AI on knowledge worker productivity and quality: Harvard Business School Technology & Operations Management Unit Working Paper No. 24-013. 2023. URL: https://ssrn.com/abstract=4573321 (дата звернення: 15.01.2026)

4. Kosmyna, N., Hauptmann, E., Yuan, Y. T., Situ, J., Liao, X. H., Beresnitzky, A. V., ... & Maes, P. Your brain on ChatGPT: Accumulation of cognitive debt when using an AI assistant for essay writing task. 2025. URL: https://arxiv.org/abs/2506.08872 (дата звернення: 15.01.2026)

5. Noy, S., & Zhang, W. Experimental Evidence on the Productivity Effects of Generative AI. 2023. URL: https://www.science.org/doi/10.1126/science.adh2586 (дата звернення: 15.01.2026)

Толпежніков Роман,
доктор економічних наук, доцент,
професор кафедри економіки та міжнародних економічних відносин
Маріупольський державний університет

Муравський Сергій,
2 курс, третій (освітньо-науковий) рівень вищої освіти,
денна форма навчання,
ОНП «Економіка»,
Маріупольський державний університет

ФРАГМЕНТАРНИЙ ПІДХІД ДО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ ТА ЙОГО НАСЛІДКИ ДЛЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Цифрова трансформація радикально змінила профіль загроз для підприємств: інформаційні системи, хмарні сервіси, віддалена робота, платформи даних і цифрові ланцюги

постачання перетворили кіберризики на системний економічний чинник. Для бізнесу це означає, що кіберінциденти більше не є суто «IT-проблемою» – вони прямо впливають на фінансові результати, безперервність операцій, репутацію та конкурентні переваги. Світові тенденції підтверджують масштаб проблеми: частота кібератак у глобальній економіці відчутно зросла, а ризик значних втрат збільшується, створюючи потенціал суттєвих фінансових шоків навіть для великих організацій [3]. У контексті глобальних загроз кіберзлочинність та кібервразливість входять до групи найбільш значущих ризиків найближчого десятиліття [5], що підкреслює стратегічний характер кібербезпеки для економічної безпеки підприємств.

Разом із тим на практиці поширеним є фрагментарний підхід до управління кібербезпекою – ситуація, коли захист вибудовується як сукупність розрізнених технічних рішень і локальних заходів без узгодженої стратегії, інтеграції в корпоративне управління та систему економічної безпеки. Ознаками фрагментарності є: відокремлення кібербезпеки від загальної системи економічної безпеки та ризик-менеджменту, домінування техноцентричних інструментів над організаційними й процесними практиками, реактивність (переважання реагування «після факту» над попередженням). Емпіричною ілюстрацією масштабу фрагментації є дані про надмірну кількість засобів захисту в організаціях (десятки продуктів від десятків постачальників), що ускладнює контроль, знижує прозорість та збільшує витрати на управління безпекою [1]. У підсумку фрагментарність перетворюється на самостійну економічну проблему: створює додаткові трансакційні витрати, підвищує ймовірність інцидентів та збільшує їхні наслідки.

Економічна безпека підприємства трактується як стан захищеності ресурсів і здатності до стійкого функціонування та розвитку за умов впливу внутрішніх і зовнішніх загроз. У цифровій економіці інформаційні активи (дані, програмні середовища, цифрові процеси, інтелектуальна власність) стають ключовими ресурсами, а тому кібербезпека – необхідною умовою підтримання економічної безпеки. Міжнародні підходи наполягають на тому, що цифрова безпека має розглядатися не лише як технічний ризик, а як економічний і соціальний ризик, інтегрований у прийняття управлінських рішень. Відповідно, управління кіберризиками має бути частиною загальної системи управління ризиками підприємства, із залученням вищого керівництва та визначенням прийнятного рівня ризику [4].

Фрагментарний підхід можна визначити як несистемне управління кібербезпекою, за якого рішення щодо захисту приймаються локально (під конкретні інциденти або вимоги), без єдиної архітектури контролів, узгоджених політик, прозорої моделі відповідальності та інтеграції із бізнес-цілями. Такий підхід часто має короткострокову логіку «закрити вразливість – купити інструмент – перейти до наступної проблеми», що породжує

накопичення неузгоджених засобів. Дослідження практик «платформізацій» у кібербезпеці показує, що саме фрагментація обмежує здатність організацій ефективно протидіяти загрозам і підвищує складність керування [1].

Ключові причини поширення фрагментарності пов'язані з поєднанням організаційних і контекстних чинників. Діє інституційна інерція: історично кібербезпеку закріплюють за IT-функцією, а залучення вищого менеджменту та інтеграція з корпоративним управлінням залишаються недостатніми. Також, домінує техноцентрична парадигма, коли безпеку сприймають передусім як набір інструментів, а не як систему процесів, правил, відповідальності та культури. Крім того, значну роль відіграє реактивність, зумовлена дефіцитом компетенцій і ресурсів: інвестиції у захист часто здійснюються постфактум – після інцидентів, а не на основі проактивної стратегії. Наостанок, складність регуляторного та технологічного середовища і багатокомпонентність IT-ландшафтів спонукають до точкових рішень «під конкретну проблему», що підсилює фрагментацію.

Фрагментарне управління кібербезпекою підриває економічну безпеку через підвищення ймовірності інцидентів і зростання сукупної вартості їх наслідків. Воно збільшує прямі витрати на відновлення та правове врегулювання, а також накопичує приховані втрати, пов'язані з управлінською складністю, дублюванням інструментів і зниженням продуктивності. Дослідження вказують на зростання ризику «екстремальних» збитків від кіберінцидентів [3] і масштабні глобальні економічні втрати від кіберзагроз, причому значна частина шкоди часто проявляється як простій, відтік клієнтів і падіння доходів [2].

Розрізнені засоби захисту знижують прозорість загроз і ускладнюють координацію реагування, що подовжує час виявлення та локалізації атак і підвищує ризики зупинок операцій. На цьому тлі інтеграція й консолідація інструментів скорочують час виявлення та реагування і зменшують економічні наслідки інцидентів [1], тоді як фрагментарність дає протилежний ефект.

Фрагментарний підхід також посилює репутаційні та регуляторні ризики. Витоки даних і публічні інциденти підривають довіру, провокують штрафи та судові витрати і створюють довгостроковий тиск на ринкові позиції й вартість залучення ресурсів адже кіберінциденти також порушують довіру до підприємства [3]. У стратегічній площині фрагментарність ускладнює безпечну цифрову трансформацію, підвищує ризик компрометації інтелектуальної власності та переводить управління в режим ліквідації наслідків замість розвитку.

Системний підхід до кібербезпеки означає інтеграцію кіберризиків у системи прийняття рішень і економічну безпеку, перехід від реактивності до проактивності, стандартизацію та узгодження політик, поєднання технологічних, організаційних і кадрових заходів. Нормативно-методичним підґрунтям для такого підходу виступають міжнародні рамки та

стандарти, зокрема ISO або NIST щодо інтеграції кіберризику в систему управління ризиками підриємства.

Фрагментарний підхід мінімізує витрати в короткостроковій перспективі, але збільшує очікувані втрати від інцидентів, послаблює прозорість і керованість, створює приховані витрати. Системний підхід потребує інституційних змін, однак зменшує складність, пришвидшує реагування та підвищує рівень економічної безпеки.

Література

1. International Business Machines (IBM) Institute for Business Value та Palo Alto Networks, 2025. Capturing the cybersecurity dividend: How security platforms generate business value. URL: https://www.ibm.com/thought-leadership/institute-business-value/en-us/report/unified-cybersecurity-platform (дата звернення: 18.01.2026)
2. International Business Machines (IBM) та Ponemon Institute, 2025. Cost of a Data Breach Report. URL: https://www.ibm.com/reports/data-breach (дата звернення: 18.01.2026)
3. International Monetary Fund, 2024. Rising Cyber Threats Pose Serious Concerns for Financial Stability. URL: https://www.imf.org/en/blogs/articles/2024/04/09/rising-cyber-threats-pose-serious-concerns-for-financial-stability (дата звернення: 18.01.2026)
4. Quinn, S., Chua, J., Ivy, N., Gardner, R. K., Scarfone, K., Smith, M. C., Witte, G., 2025. Integrating Cybersecurity and Enterprise Risk Management (ERM). *National Institute of Standards and Technology Interagency Report*, NIST IR 8286r1. DOI: 10.6028/NIST.IR.8286r1
5. World Economic Forum, 2023. The Global Risks Report 2023. 18th Edition. URL: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf (дата звернення: 18.01.2026).