Сліпченко Т.О.
доцент кафедри безпеки та правоохоронної діяльності,
Західноукраїнський національний університет
Блащук А. В.
студентка ПДЕБ-21 юридичного факультету,
Західноукраїнський національний університет

ІНФОРМАЦІЙНА ПІДТРИМКА ПРИЙНЯТТЯ УПРАВЛІНСЬКИХ РІШЕНЬ У СФЕРІ ЕКОНОМІЧНОЇ БЕЗПЕКИ

У сучасних реаліях, що характеризуються високим рівнем невизначеності та тривалою воєнною агресією, проблема забезпечення економічної безпеки України трансформується з площини статичного захисту ресурсів у площину динамічного управління ризиками. Згідно з дослідженнями Національного інституту стратегічних досліджень (2024 р.), ключовими викликами для суб'єктів господарювання залишаються різкий економічний спад та необхідність адаптації до умов довготривалої війни, що потребує миттєвої реакції управлінського апарату.

У таких умовах інформація стає не просто допоміжним ресурсом, а стратегічним базисом для антикризових рішень. Цифрова трансформація 2023–2025 років докорінно змінила підходи до інформаційної підтримки: впровадження систем на основі Big Data та штучного інтелекту дозволяє не лише моніторити поточні аномалії, а й прогнозувати потенційні загрози (фрод, кіберінциденти, логістичні розриви) ще до їх настання.

Проте стрімка диджиталізація створює і нові вразливості. Інформаційна підтримка сьогодні стикається з викликами «інформаційного шуму», кіберзагроз та необхідністю інтеграції розрізнених даних у єдині ситуаційні центри управління. Відтак, розробка ефективного механізму інформаційної підтримки прийняття управлінських рішень є критично

важливою для зміцнення стійкості як окремих підприємств, так і національної економіки в цілому.

Теоретичний фундамент інформаційної підтримки економічної безпеки в сучасних умовах пройшов трансформацію від простого накопичення звітних даних до розбудови когнітивних систем управління. Згідно з актуальними дослідженнями 2023–2024 років, інформація розглядається як «імунна система» суб'єкта господарювання, яка забезпечує його адаптивність до шокових впливів. Сьогодні інформаційна підтримка включає не лише фінансовий моніторинг, а й глибокий аналіз неструктурованих даних: від політичних декларацій та змін у митному законодавстві до аналізу тональності соціальних мереж. Науковий дискурс останніх двох років змістився в бік «інформаційної резистентності» — здатності системи виявляти цілеспрямовані вкиди та маніпуляції, спрямовані на дестабілізацію економічного стану. Це вимагає від архітектури безпеки використання багаторівневих моделей класифікації джерел, де пріоритет надається перехресній верифікації даних з незалежних каналів, що дозволяє сформувати об'єктивне підґрунтя для стратегічного планування.

Практичний механізм прийняття рішень у 2024–2025 роках базується на інтеграції технологій штучного інтелекту (AI) та великих даних (Big Data) у контур управління безпекою. Процес починається з безперервного сканування внутрішнього та зовнішнього середовища, де алгоритми машинного навчання ідентифікують патерни потенційних загроз — від нетипових фінансових транзакцій до аномалій у поведінці контрагентів. Використання сучасних систем класу Business Intelligence (BI) дозволяє візуалізувати ризики у форматі динамічних дашбордів, що критично важливо для топменеджменту в умовах дефіциту часу. Особливу роль відіграє предиктивна аналітика: замість констатації збитків, система моделює ймовірні сценарії розвитку кризи (наприклад, оцінка впливу

чергового блекауту або зміни валютного курсу на платоспроможність компанії). Такий підхід перетворює інформаційне забезпечення на інструмент проактивного маневрування, де управлінське рішення приймається на основі математично обґрунтованого прогнозу, а не лише інтуїції керівника.

Аналіз сучасних викликів свідчить, що головним бар'єром для ефективної інформаційної підтримки у 2025 році є «парадокс доступності»: за надлишку даних спостерігається дефіцит змістовної інформації для прийняття рішень. Критичною проблемою залишається технологічний розрив між швидкістю виникнення кіберзагроз та швидкістю оновлення захисних систем аналітики. Досвід українських підприємств показує, що цифровізація без належного захисту даних створює ризики «цифрового захоплення» бізнесу через витік комерційної таємниці. Перспективи вирішення цих проблем лежать у впровадженні архітектури Zero Trust (нульової довіри) та використанні блокчейн-технологій для забезпечення незмінності аудиторського сліду управлінських рішень. Майбутнє сфери пов'язане з автоматизацією не лише збору, а й інтерпретації даних за допомогою великих мовних моделей (LLM), адаптованих під специфіку економічної безпеки, що дозволить мінімізувати людський фактор та корупційні ризики на етапі підготовки аналітичних записок.

ЛІТЕРАТУРА:

1. Захаров О. І. Цифрова трансформація системи економічної безпеки підприємства в умовах воєнного стану. *Економіка та суспільство*. 2024. Вип. 61. URL: economyandsociety.in.ua.

2. Іванова В. В. Роль штучного інтелекту в інформаційному забезпеченні прийняття управлінських рішень. *Менеджмент та підприємництво в Україні: етапи становлення і проблеми розвитку*. 2023. Вип. 5. С. 42–49.

3. Копитко М. І. Інформаційна безпека як домінанта зміцнення економічної стійкості суб'єктів господарювання. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2024. Вип. 1. С. 12–21.

4. Мельник О. Г. Моделювання сценаріїв прийняття рішень на основі Big Data в системі економічної безпеки. *Бізнес Інформ*. 2023. № 11. С. 156–163.

5. Прокопенко О. В. Інноваційні інструменти інформаційної підтримки антикризового управління. *Економічний вісник НТУУ «КПІ»*. 2024. Вип. 28. С. 88–95.

6. Ситник Г. В. Державна політика забезпечення економічної безпеки України в умовах глобальних трансформацій: аналітична доповідь. *Національний інститут стратегічних досліджень*. 2024. 45 с.

7. Шевченко А. М. Кіберстійкість інформаційних систем управління як складник економічної безпеки бізнесу. *Кібербезпека: освіта, наука, техніка*. 2025. Т. 1. № 23. С. 104–112.