8.2. Роль інновацій і цифрових технологій у забезпеченні економічної безпеки: метасценарне та input-output моделювання

Маслак О.І.,
доктор економічних наук, професор, завідувачка кафедри економіки,
Яковенко Я.Ю.,
PhD з економіки, доцент кафедри економіки,
Доманецький І.В.,
здобувач PhD,
Кременчуцький національний університет
імені Михайла Остроградського

Ключові слова: економічна безпека, цифрові технології, моделювання, інновації, input-output модель, метасценарії

Інновації та цифрові технології відіграють ключову роль у трансформації бізнес-середовища та забезпеченні економічної безпеки України. Знизити витрати, підвищити рівень захисту інформації та поліпшити доступ до фінансових ресурсів – перспективні задачі, що потребують швидких рішень, особливо в умовах воєнного стану, коли швидке реагування на зміни у зовнішньому середовищі, підвищує стійкість бізнесу до кризових явищ.

За даними оцінки впливу війни на мікро-, малі та середні підприємства в Україні, розробленої Центром економічного відновлення (CER) [8], протягом 2022-2023 років, попри воєнні дії, спостерігалося зростання використання цифрових технологій серед українських підприємств на понад 15%, що свідчить про активну адаптацію бізнесу до нових реалій. При цьому IT-індустрія є найбільш мобільним сектором: чверть компаній або повністю переміщені, або відкривають додаткові офіси та філії в західному регіоні країн. До числа лідерів за темпами імплементації належать послуги хмарних сервісів, систем кібербезпеки та онлайн-платформ для управління ланцюгами постачання [7].

Крім того, цифрові технології сприяють підвищенню ефективності роботи банків, зокрема, шляхом зниження операційних витрат та прискорення обробки фінансових операцій, адже світовий і вітчизняний досвід показує, що нові цифрові технології швидше сприймаються і впроваджуються в фінансовому та банківському секторі, які є лідерами цифрової трансформації в країні. Таким чином, інновації та цифрові технології формують основу для забезпечення економічної безпеки України через оптимізацію бізнес-процесів, автоматизацію та впровадження нових бізнес-моделей у різних секторах економіки.

Водночас умовах нестабільності та невизначеності особливо важливим стає прогнозування майбутніх сценаріїв розвитку економіки. Саме тому, для

ефективного планування та забезпечення економічної безпеки необхідним інструментом виступає розробка метасценаріїв – окремих сценаріїв розвитку економічної безпеки з унікальними характеристиками та вихідними даними (рис. 1).

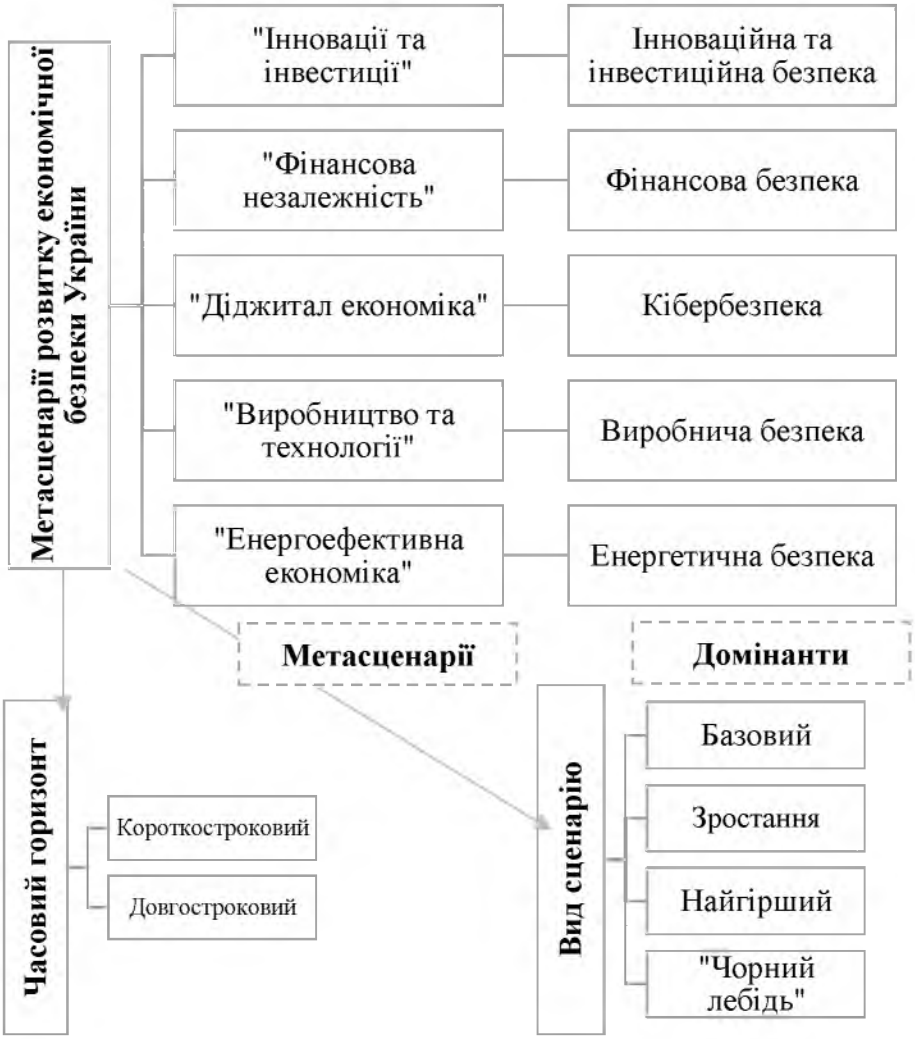

Рис. 1. – Система метасценаріїв розвитку економічної безпеки України
Джерело: розроблено авторами на основі [5, 6, 10]

Структурно система метасценаріїв розвитку економічної безпеки України включає такі складові як власне метасценарії, домінанти метасценаріїв, часовий горизонт прогнозів та вид сценарію. Виходячи з того, що економічна безпека визначається як стан захищеності національних економічних інтересів від зовнішніх і внутрішніх загроз [11], інновації та цифрові технології впливають на економічну безпеку через: технологічну конкурентоспроможність (інновації сприяють розвитку нових галузей та підвищенню продуктивності) і інформаційну безпеку (цифрові технології забезпечують захист критичної інформації); соціальну стабільність (інновації створюють нові робочі місця та покращують якість життя).

Аналізуючи запропоновані метасценарії, слід відзначити, що, зважаючи на фактори, які значним чином впливатимуть на економічну безпеку України в майбутньому (енергетичні, виробничі, діджитал, фінансові чи інноваційно-інвестиційні), кожен сценарій надає вирішальну роль саме цьому ключовому фактору. Відповідно, інші види економічної безпеки також включаються у сценарій, проте з меншим впливом. Коротка характеристика метасценаріїв включає наступні припущення:

- «Енергоефективна економіка» – важливий метасценарій розвитку економічної безпеки України, який базується на такому припущенні, що енергетична сфера є пріоритетною та визначає поточний стан економічної безпеки загалом. Відповідно, показники розвитку енергетичної сфери є визначальними для реалізації даного метасценарію;

- «Виробництво та технології» – основною гіпотезою даного метасценарію є теза про те, що виробництво є рушійною силою економіки та зростання рівня економічної безпеки. Відповідно, технології та виробництво відіграють провідну роль у розвитку економічної безпеки загалом;

- «Діджитал економіка» – пріоритетну роль у розвитку економічної безпеки України відіграватиме діджиталізація економіки та кібербезпека. Відповідно, ІТ-сектору надається найбільша вага серед усх інших секторів економіки України;

- «Фінансова незалежність» – базується на гіпотезі, що власні фінансові ресурси та зниження державного боргу впливають на всі інші види економічної безпеки;

- «Інновації та інвестиції» – даний метасценарій передбачає, що інноваційно-інвестиційний розвиток є пріоритетом економічної безпеки країни.

Результати метасценарного моделювання показують, що сценарії з високим рівнем впровадження інновацій та цифрових технологій характеризуються вищою економічною безпекою. Однак, ці сценарії також вимагають значних інвестицій в інфраструктуру та людський капітал, а цифровізація, хоч і сприяє зміцненню зв'язків між секторами економіки, але також може збільшити вразливість до кібератак.

Варто зазначити, що важливою складовою впливу інновацій на економічну безпеку є також посилення кібербезпеки. Захист конфіденційної інформації, попередження кібератак та створення ефективних протоколів реагування на загрози є критичними для стабільного функціонування економіки. Інвестиції в розвиток кіберзахисту дозволяють забезпечити безперебійну роботу цифрових платформ і зберегти довіру споживачів.

За прогнозами світові збитки від кіберзлочинності до 2025 року можуть сягнути 10 трильйонів доларів [8]. У звіті підкреслюється, що кіберзлочинність є однією з найбільших загроз для світової економіки, і ця проблема особливо актуальна для України в умовах війни.

Активізація кібератак на критичну інфраструктуру вимагає негайного впровадження сучасних систем захисту. За даними Держспецзв'язку [2] у 2024 році кількість кібератак на Україну зросла майже на 70% у порівнянні з 2023 роком. При цьому кількість кібератак на державні установи та підприємства критичної інфраструктури (енергетика, оборона) зросла більш ніж удвічі у першому півріччі 2024 року.

Відповідно, для більш точного аналізу та управління ризиками, пов'язаними з економічною безпекою, необхідно використовувати сучасні інструменти, такі як сценарне моделювання.

В умовах воєнних дій, та руйнувань критичної інфраструктури пропонується використовувати 4 основні види сценаріїв, що включають:

1) базовий сценарій – передбачає зміну показників (що визначають економічну безпеку) у невеликих масштабах (5-10% річної зміни), що не впливає значним чином на загальний результат розвитку системи;

2) сценарій зростання – передбачає зростання темпів розвитку для показників-стимуляторів та, відповідно, зниження для показників-дестимуляторів (у межах більше 10% річної зміни);

3) найгірший сценарій – основним припущенням є зниження темпів розвитку для показників-стимуляторів та, відповідно, збільшення негативних тенденцій для показників-дестимуляторів (у межах більше 10% річної зміни);

4) «чорний лебідь» – базується на гіпотезі, що в межах прогнозованого часового горизонту трапляються нетривіальні події (пандемія, війна), які значним чином впливають на всі економічні показники.

Крім того, важливим аспектом оцінювання є аналіз функціональних компонент економічної безпеки, таких як фінансова, інвестиційна, зовнішньоекономічна безпека тощо. Такий підхід дозволяє детально дослідити окремі аспекти економічної безпеки та виявити потенційні загрози в кожній з них. При цьому, важливо використовувати як кількісні, так і якісні показники . Кількісні показники, такі як фінансові коефіцієнти, дозволяють об'єктивно оцінити стан економіки, в той час як якісні показники, такі як експертні оцінки, враховують суб'єктивні фактори та думки фахівців.

Для прогнозування майбутніх ризиків та можливостей для економічної безпеки використовується форсайт-аналіз. Цей метод дозволяє передбачити потенційні загрози та розробити стратегії для їх запобігання. Експертні

опитування також є важливим інструментом для оцінки ризиків та розробки рекомендацій. Залучення експертів дозволяє врахувати різні точки зору та отримати більш об'єктивну оцінку ситуації.

Ще один метод аналізу, що дозволяє досліджувати взаємозв'язки між різними секторами економіки – це input-output моделювання, що зокрема може бути використано для:

1) аналізу впливу інновацій на різні сектори економіки (дослідження того, як впровадження нових технологій впливає на виробництво, зайнятість та інші економічні показники в різних секторах);

2) оцінки впливу зовнішніх шоків на економіку (аналіз того, як зміни у світовій економіці, цінах на ресурси, політичній ситуації впливають на різні сектори економіки та економічну безпеку в цілому);

3) розробки стратегій розвитку економіки (визначення пріоритетних секторів для інвестицій та розвитку, з метою підвищення економічної безпеки та стійкості).

У якості ілюстрації того, наскільки складними є взаємозв'язки між різними аспектами економічної безпеки України, пропонуємо детальніше розглянути input-output модель "Енергоефективна економіка" (рис. 2).

Наведена модель окреслює, як різні фактори впливають на енергетичну безпеку та як цей вплив трансформується в результаті взаємодії. Зважаючи на нинішню ситуацію, енергетична безпека має надважливе значення для України, адже внаслідок постійних атак на енергетичну інфраструктуру, Україна втратила біля 50% генерації електроенергії. Руйнування енергетичної інфраструктури вимагає пошуку нових, енергоефективних рішень для відновлення економіки. Запропонована input-output модель дозволяє оцінити ефективність різних сценаріїв відновлення енергетичної інфраструктури та вибрати найбільш оптимальний.

Як бачимо із запропонованої моделі, першочерговим є визначення вхідних даних, які є рушійними силами змін в енергетичному секторі (включає в себе зниження боргів населення за енергоносії та встановлення справедливих тарифів, що забезпечує соціальну справедливість та фінансову стабільність; важливу роль відіграє також соціальна безпека, яка передбачає захищену та інноваційну енергетику, а також зміну структури інвестицій).

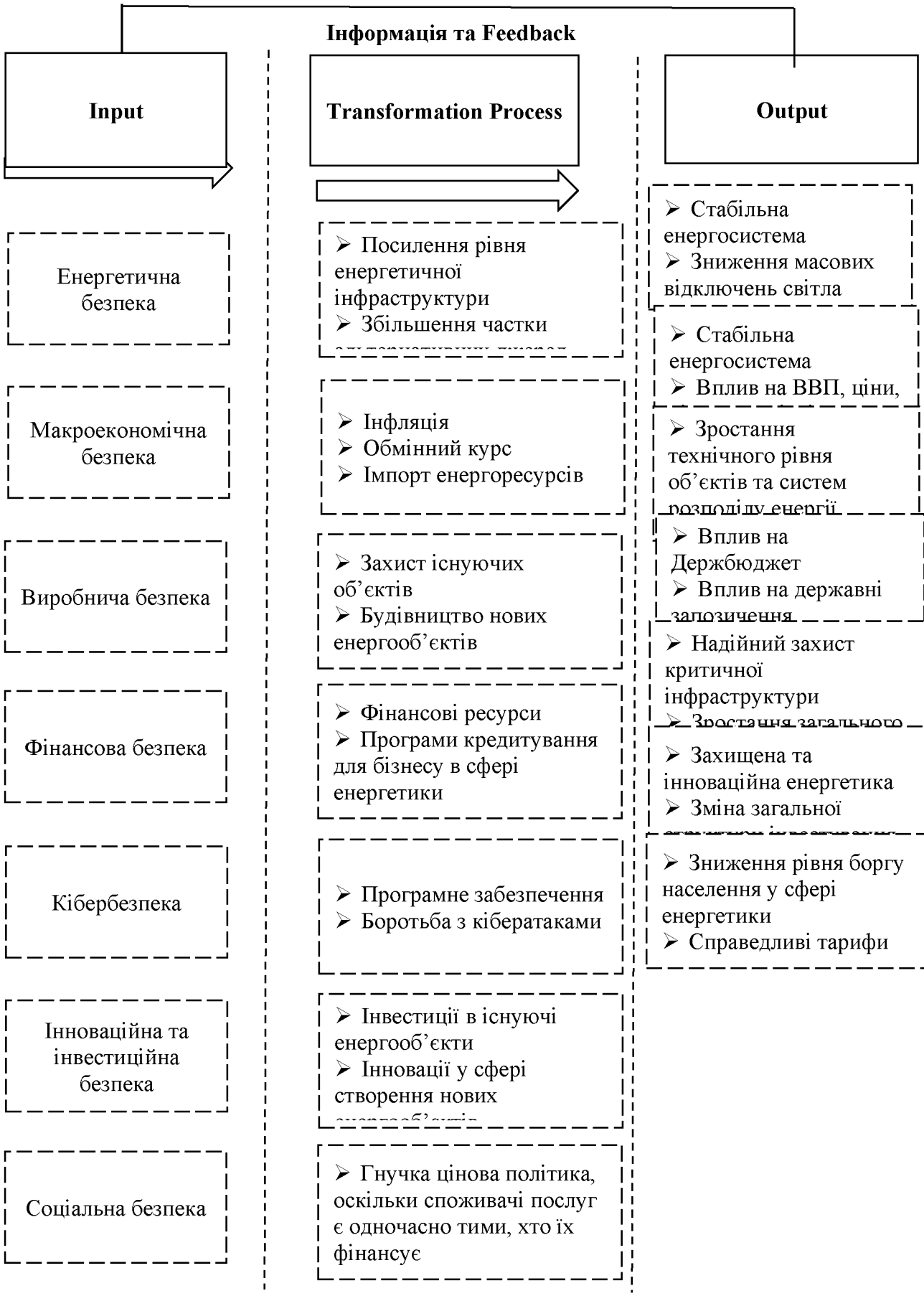

Рис. 2. – Input-output модель метасценарію «Енергоефективна економіка»

Джерело: узагальнено авторами на основі [1, 3, 9]

При цьому інноваційна та інвестиційна безпека є ключовими факторами трансформації (включають в себе захист критичної інфраструктури та підвищення кібербезпеки, що є особливо актуальним в умовах цифрової трансформації).

Впровадження інноваційних рішень в енергетиці є ключовим фактором для досягнення енергоефективності та сталого розвитку. Мається на увазі використання новітніх технологій для виробництва енергії з відновлюваних джерел, таких як сонячна та вітрова енергія, а також впровадження "розумних мереж" (Smart Grids) для оптимізації розподілу електроенергії. Фінансова безпека, в свою чергу, забезпечує модернізацію енергетичної інфраструктури та стабільну роботу атомних електростанцій.

Виробнича безпека гарантує захист існуючих енергетичних об'єктів та будівництво нових, що сприяє розвитку енергетичного сектору. Макроекономічна безпека враховує вплив інфляції, обмінного курсу та імпорту енергоресурсів на енергетичну систему.

Усі наведені фактори взаємодіють в процесі трансформації, який призводить до певних результатів. Стабільна енергосистема та зниження кількості відключень електроенергії є основними цілями моделі. Крім того, вона передбачає зростання кібербезпеки, зміну структури інвестицій та вплив на державний бюджет. Модель також враховує вплив на макроекономічні показники, такі як ВВП, ціни та рівень торгівлі. В цілому, input-output модель "Енергоефективна економіка" не лише окреслює взаємозв'язки між різними аспектами економічної безпеки, але й підкреслює важливу роль інновацій та цифрових технологій у трансформації бізнесу, особливо в енергетичному секторі.

Важливо зазначити, що цифрові технології відіграють важливу роль у трансформації бізнес-процесів в енергетичній галузі. Використання Інтернету речей (IoT) дозволяє збирати та аналізувати дані про роботу енергетичної інфраструктури в режимі реального часу, що сприяє підвищенню ефективності та своєчасному виявленню проблем, а штучний інтелект (AI) може бути використаний для прогнозування попиту на електроенергію, оптимізації роботи енергетичних ринків та автоматизації процесів управління енергосистемами.

Крім того, впровадження цифрових технологій також сприяє підвищенню прозорості та ефективності взаємодії між енергетичними компаніями та споживачами. Наприклад, онлайн-платформи дозволяють споживачам контролювати своє споживання енергії, отримувати інформацію про тарифи та здійснювати платежі в режимі онлайн, а сучасна концепція "енергетичного просьюмерства" передбачає, що споживачі можуть не лише споживати, але й

виробляти електроенергію, використовуючи власні сонячні панелі або інші відновлювані джерела енергії [4].

Таким чином, інновації та цифрові технології є не лише інструментами для досягнення енергетичної безпеки, але й рушійними силами трансформації бізнесу в енергетичному секторі, сприяючи його сталому розвитку та підвищенню конкурентоспроможності. Їх впровадження та розвиток сприяють підвищенню конкурентоспроможності, диверсифікації економіки та створенню нових можливостей для зростання.

Економічна безпека в епоху цифровізації вимагає комплексного та стратегічного підходу, що враховує складні взаємозв'язки між технологіями, економікою та суспільством. Синергія інновацій та цифрових технологій є ключовим фактором забезпечення стійкості економічних систем. Інновації створюють нові можливості для розвитку, підвищують конкурентоспроможність та стимулюють економічне зростання. Цифрові технології, у свою чергу, забезпечують ефективне використання цих можливостей, оптимізують виробничі процеси, покращують якість послуг та створюють нові ринки.

Однак, без стратегічного підходу та належного регулювання, цифрові технології можуть також створювати нові загрози, такі як кіберзлочинність, цифрова нерівність та залежність від технологічних монополій. Одночасно, необхідно мінімізувати потенційні ризики, пов'язані з цифровізацією. Це вимагає розробки комплексних стратегій кібербезпеки.

Для ефективного аналізу ролі інновацій та цифрових технологій у забезпеченні економічної безпеки, необхідні сучасні аналітичні інструменти. Метасценарне та input-output моделювання є важливими складовими цього аналітичного арсеналу. Метасценарне моделювання дозволяє розглянути різні сценарії розвитку технологій та економіки, оцінити їх потенційний вплив на економічну безпеку та розробити стратегії реагування на можливі загрози. Input-output моделювання, у свою чергу, дозволяє аналізувати взаємозв'язки між різними секторами економіки, оцінити вплив технологічних змін на ці взаємозв'язки та виявити потенційні вразливості.

Обидва методи дозволяють враховувати широкий спектр факторів, включаючи технологічні, економічні, соціальні та політичні. Вони дають можливість оцінити прямі та непрямі наслідки впровадження інновацій та цифрових технологій, а також виявити потенційні ризики та можливості. Використання цих методів дозволяє приймати обґрунтовані рішення щодо державної політики у сфері економічної безпеки.

Однак, важливо пам'ятати, що метасценарне та input-output моделювання є лише інструментами, а не панацеєю. Їх ефективність залежить від якості даних,

точності моделей та здатності аналітиків інтерпретувати результати. Тому, необхідно постійно вдосконалювати ці методи, розробляти нові підходи до аналізу даних та підвищувати кваліфікацію аналітиків.

Список використаних джерел:

1.Гаврилюк, І., Клят, Ю., Семененко, Л., Добровольський, Ю., Сеченєв, О. (2025). Щодо основних положень оцінювання та прогнозування рівня воєнно-економічної безпеки держави. In the 4th International scientific and practical conference "Development of higher education: trends and prospects"(January 28–31, 2025) Rotterdam, Netherlands. International Science Group. 2025. 250 p. (p. 22).

2. Державна служба спеціального зв'язку та захисту інформації України. Офіційний сайт. URL: https://cip.gov.ua/ua

3. Жукова, Ю. М., Юрченко, О. А., Василенко, В. (2024). Стратегії забезпечення економічної безпеки країни в умовах глобальних викликів. Вісник Хмельницького національного університету. Серія: Економічні науки, 328(2), 401-409.

4. Касич А.О., Яковенко Я.Ю. Газові ринки ЄС та України: сучасний стан і перспективи розвитку. Бізнес Інформ. 2013. № 9ю С. 8-15. URL: http://nbuv.gov.ua/UJRN/binf_2013_9_2

5. Квашук Д.М. (2017). Моделювання інформаційно-аналітичного забезпечення економічної безпеки промислових підприємств в умовах посилення інтеграційних процесів. Економіка та суспільство, 4(12), 2017.

6. Лупак, Р. Л., Наконечна, Н. В. Сценарії формування резервів підвищення економічної ефективності підприємств сфери послуг з орієнтацією на інноваційний розвиток. Innovation and Sustainability.. 2024 - № 1: с.43-49.

7. Неустроєв, Ю. Г Роль інформаційних технологій у забезпеченні економічної безпеки країни. Інвестиції: практика та досвід, 2021. - №8, с.40-44.

8. Оцінка впливу війни на мікро-, малі та середні підприємства в Україні. Київ: Програма розвитку ООН в Україні, 2024 рік. URL: https://surl.li/cdyrcr

9. Цаль-Цалко, Ю. Формування економічних індикаторів національної безпеки в умовах цифровізації бізнесу та змін в економіці. Society and Security, 2024. - №(1 (2)), 3-13.

10. Яковенко, Я., Доманецький, І. Нормативно-правове регулювання економічної безпеки країни: сучасний стан та перспективи розвитку. Цифрова економіка та економічна безпека, 2024. - №(6(15), с.86-93. https://surl.li/pvozjs

11. Maslak, O., & Grishko, N. (2013). Management of economic safety of the enterprise on the principles of ensuring its rational level. Management and marketing of innovations, (1), 198-208.