ECONOMIC BULLETIN
of Cherkasy State Technological University Vol. 26. Issue 2(75)2025 141–153

UDC 330.341.1:330.322:004.9 (477)
DOI: 10.24025/2306-4420.75(2).2025.338600

JEL Classification Code: O3, E22
Article's History:
Received:21.03.2025; Revised: 31.03.2025; Accepted: 11.04.2025.

Oleksii Hutsaliuk*
Doctor of Economics, Professor
Private Higher Education Institution
"Rauf Ablyazov East European University"
18036, 16 Nechuya-Levytskyi St., Cherkasy, Ukraine
https://orcid.org/0000-0002-6541-4912

Iuliia Bondar
PhD, Associate Professor
Volodymyr Vynnychenko Central Ukrainian State University
25006, 1 Shevchenko St., Kropyvnytskyi, Ukraine
https://orcid.org/0000-0003-2269-6208

Iia Chudaieva
Doctor of Economics, Professor
Private Higher Education Institution
"Rauf Ablyazov East European University"
18036, 16 Nechuya-Levytskyi St., Cherkasy, Ukraine
https://orcid.org/0000-0001-7759-2372

Galyna Us
Doctor of Economics, Professor
Private Higher Education Institution
"Rauf Ablyazov East European University"
18036, 16 Nechuya-Levytskyi St., Cherkasy, Ukraine
https://orcid.org/0000-0001-8954-591X

Transformation processes in strategising the innovation and investment potential of the national economy in the coordinates of information changes and protection of state interests

Abstract. The article examines transformation processes in strategising the innovation and investment potential of the national economy in the context of profound information changes and the need to protect state interests. It is emphasised that digitalisation, the development of information and communication technologies, artificial intelligence, big data and blockchain create new opportunities for economic growth, but at the same time generate risks associated with cyber threats, the vulnerability of critical infrastructure and the loss of control over strategic resources. In this context, the state's innovation and investment policy, aimed at the creation of a favourable environment for attracting capital to high-tech sectors, the formation of national digital platforms and the development of a cyber resilience system, acquires special importance. Systemic, structural-functional, institutional and comparative approaches, which allowed for a comprehensive assessment of the relationships between innovation processes, investment mechanisms

*Corresponding author

and digital transformations, became the methodological basis of the study. The scientific novelty of the work lies in the development of a model for strategising the innovation and investment potential in the coordinates of the information economy, which combines the priorities of digital development with the requirements of national security. The results of the study can be used to improve state policy in the field of innovation, investment and digital transformation, as well as to form effective mechanisms for protecting strategic interests of the state in the context of global competition

Keywords: digitalisation, state innovation policy, investment mechanisms, national security, cyber resilience, strategic interests of the state

Олексій Гуцалюк
Доктор економічних наук, професор
Приватний заклад вищої освіти
«Східноєвропейський університет імені Рауфа Аблязова»
18036, вул. Нечуя-Левицького, 16, м. Черкаси, Україна
https://orcid.org/0000-0002-6541-4912

Юлія Бондар
Кандидат економічних наук, доцент
Центральноукраїнський державний університет
імені Володимира Винниченка
25006, вул. Шевченка, 1, м. Кропивницький, Україна
https://orcid.org/0000-0003-2269-6208

Ія Чудаєва
Доктор економічних наук, професор
Приватний заклад вищої освіти
«Східноєвропейський університет імені Рауфа Аблязова»
18036, вул. Нечуя-Левицького, 16, м. Черкаси, Україна
https://orcid.org/0000-0001-7759-2372

Галина Ус
Доктор економічних наук, професор
Приватний заклад вищої освіти
«Східноєвропейський університет імені Рауфа Аблязова»
18036, вул. Нечуя-Левицького, 16, м. Черкаси, Україна
https://orcid.org/0000-0001-8954-591X

Трансформаційні процеси в стратегуванні інноваційно-інвестиційного потенціалу національної економіки в координатах інформаційних змін та захисту інтересів держави

Анотація. У статті розглянуто трансформаційні процеси в стратегуванні інноваційно-інвестиційного потенціалу національної економіки в умовах глибоких інформаційних змін та необхідності захисту державних інтересів. Підкреслюється, що цифровізація, розвиток інформаційно-комунікаційних технологій, штучного інтелекту, великих даних і блокчейну формують нові можливості для економічного зростання, але водночас породжують ризики, пов’язані з кіберзагрозами, вразливістю критичної інфраструктури та втратою контролю над стратегічними ресурсами. У цьому контексті особливого значення набуває інноваційно-інвестиційна політика держави, спрямована на створення сприятливого середовища для залучення капіталу у високотехнологічні сфери, формування

національних цифрових платформ і розбудову системи кіберстійкості. Методологічною основою дослідження стали системний, структурно-функціональний, інституційний та порівняльний підходи, що дозволили комплексно оцінити взаємозв'язки між інноваційними процесами, інвестиційними механізмами та цифровими трансформаціями. Наукова новизна роботи полягає у розробленні моделі стратегування інноваційно-інвестиційного потенціалу в координатах інформаційної економіки, яка поєднує пріоритети цифрового розвитку з вимогами національної безпеки. Результати дослідження можуть бути використані для удосконалення державної політики у сфері інновацій, інвестицій та цифрової трансформації, а також для формування ефективних механізмів захисту стратегічних інтересів держави в умовах глобальної конкуренції

Ключові слова: цифровізація, державна інноваційна політика, інвестиційні механізми, національна безпека, кіберстійкість, стратегічні інтереси держави

Вступ

Сучасний етап розвитку національної економіки характеризується динамічними трансформаціями, зумовленими глобалізаційними процесами, прискореною цифровізацією та зростанням ролі інформаційних ресурсів у створенні доданої вартості. У цих умовах стратегування інноваційно-інвестиційного потенціалу набуває особливого значення як ключовий чинник підвищення конкурентоспроможності країни, зміцнення її економічної безпеки та захисту національних інтересів.

В умовах поширення інформаційних технологій, розширення доступу до великих даних і розвитку цифрової інфраструктури трансформуються традиційні підходи до стратегічного управління. Це вимагає формування нових моделей розвитку, які поєднують економічні, технологічні та безпекові аспекти. Інноваційно-інвестиційний потенціал стає не лише економічною категорією, а й стратегічним інструментом забезпечення державного суверенітету, оскільки від його рівня залежить стійкість економіки до зовнішніх і внутрішніх викликів, зокрема у сфері інформаційної та кібербезпеки.

Водночас національна економіка стикається з низкою бар'єрів, серед яких – недостатня ефективність інституційного забезпечення інноваційної діяльності, фрагментарність інвестиційних стратегій, слабка інтегрованість у глобальні ланцюги створення вартості, а також високий рівень інформаційних загроз. Це актуалізує потребу у перегляді підходів до стратегування, орієнтованих на досягнення синергії між економічним розвитком і захистом національних інтересів.

Актуальність теми дослідження зумовлена необхідністю переосмислення ролі держави у формуванні сприятливого інноваційно-інвестиційного середовища, здатного забезпечити ефективне використання інформаційних ресурсів, стимулювати інновації та водночас гарантувати безпекові пріоритети. Розробка комплексних стратегій, які інтегрують інформаційні трансформації з економічними та безпековими інтересами держави, виступає передумовою побудови стійкої національної економіки.

Огляд літератури

Проблематика стратегування інноваційно-інвестиційного розвитку та його ролі у зміцненні економічної безпеки перебуває у центрі уваги багатьох вітчизняних і зарубіжних дослідників. Теоретико-методологічні засади формування інноваційного потенціалу економіки ґрунтовно висвітлюються у працях Й. Шумпетера (Schumpeter, 1942) який розглядає інновації як ключовий рушій економічного зростання, а інвестиції – як основу їхнього практичного впровадження. Ця ідея залишається центральною в розумінні інновацій як рушійної сили зростання в дослідженнях автора К. М. Копп (Корр, 2023).

Українські науковці, серед яких В. Геєць (2007), Я. Жаліло (2009), С. Онишко (2015), наголошують на значенні інноваційно-інвестиційної політики для підвищення конкурентоспроможності національної економіки та забезпечення її адаптивності до

глобальних змін. Значний внесок у дослідження інституційного середовища стратегування інноваційно-інвестиційного потенціалу зробили також праці Л. Федулової (2015), які акцентують увагу на ролі державної підтримки та розвитку інноваційних кластерів.

У контексті інформаційних трансформацій важливими є дослідження М. Кастельса (Castells, 2010), який розглядає інформаційне суспільство як нову парадигму розвитку, що визначає характер глобальної економіки.

Актуальною для цього дослідження є також література, присвячена проблемам економічної та інформаційної безпеки. Зокрема, у працях А. Гальчинського (2023) та В. Кравченка (2016) обґрунтовується потреба в інтеграції безпекових пріоритетів у стратегічні документи економічного розвитку.

Узагальнюючи наукові підходи, можна зробити висновок, що дослідження стратегування інноваційно-інвестиційного потенціалу в умовах інформаційних змін перебуває на перетині кількох наукових напрямів: економічної теорії, інноваційного менеджменту, інформаційної економіки та досліджень національної безпеки. Однак у сучасній науковій літературі недостатньо уваги приділено комплексному аналізу трансформаційних процесів, що відбуваються на перетині цих сфер, особливо в умовах глобальних інформаційних викликів і зростання потреби у захисті інтересів держави.

Мета статті полягає у дослідженні трансформаційних процесів у стратегуванні інноваційно-інвестиційного потенціалу національної економіки в умовах інформаційних змін та визначенні механізмів забезпечення захисту інтересів держави, а саме у формуванні комплексного бачення того, як цифровізація, інтеграція даних, розвиток технологій та інноваційні інвестиції можуть забезпечити стійкий економічний розвиток, ефективне управління державними ресурсами та кіберстійкість критично важливих секторів.

Матеріали та методи

У процесі підготовки статті було використано комплекс науково-методологічних підходів, що дозволили дослідити трансформаційні процеси у стратегуванні інноваційно-інвестиційного потенціалу національної економіки в умовах інформаційних змін та необхідності захисту державних інтересів.

Методологічною основою дослідження є системний підхід – для аналізу взаємозв'язків між інноваційними процесами, інвестиційними механізмами та інформаційними трансформаціями в економіці; структурно-функціональний аналіз – для визначення ролі та значення окремих складових інноваційно-інвестиційної політики; інституційний аналіз – для розкриття ролі держави у формуванні сприятливого середовища для інновацій та інвестицій зі збереженням національних інтересів; діалектичний підхід – для осмислення динамічності та суперечливості процесів цифрової трансформації та її впливу на стратегічне управління.

Результати та обговорення

Формування ефективного інноваційно-інвестиційного потенціалу національної економіки в сучасних умовах потребує врахування впливу інформаційних трансформацій, які радикально змінюють підходи до стратегування. Посилення інформаційних викликів, зокрема кіберзагроз та деструктивних інформаційних впливів, актуалізує необхідність інтеграції безпекового компонента у стратегічні документи розвитку.

О. Гуцалюк *та ін.* (2025) вважають, що інноваційно-інвестиційний потенціал слід розглядати як інтегровану характеристику, що відображає: рівень науково-технічних і технологічних можливостей економіки; обсяг і структуру інвестиційних ресурсів; інституційні умови для реалізації інновацій; рівень розвитку цифрової та інформаційної інфраструктури.

Методологічна основа стратегування має спиратися на системний, інституційний та інформаційний підходи, що дозволяє оцінювати не лише кількісні параметри розвитку, але й якісні характеристики, пов'язані з безпекою, адаптивністю та стійкістю економічних систем.

У XXI ст. відбувається зсув від індустріальної моделі до цифрової, де ключовими ресурсами стають знання, дані та інформація, що зумовлює трансформацію інвестиційних стратегій у бік підтримки стартапів, інноваційних кластерів та венчурних проєктів; посилення ролі інтелектуальної власності та нематеріальних активів у формуванні вартості; переорієнтацію бізнес-моделей на використання цифрових платформ та мережевих ефектів; зміну підходів до управління ризиками та безпекою в умовах глобальної цифровізації.

Відповідно, стратегування інноваційно-інвестиційного потенціалу має враховувати не лише традиційні економічні чинники, але й інформаційні тренди, що визначають конкурентні позиції держави на світовому ринку.

Інформаційні трансформації несуть не тільки нові можливості, а й загрози, які прямо впливають на економічну та національну безпеку, серед них: кіберзлочинність та атаки на критичну інфраструктуру; витік стратегічно важливої інформації; маніпулятивні інформаційні впливи на економічні процеси; залежність від іноземних цифрових технологій і платформ.

Захист інтересів держави вимагає створення інтегрованої системи кібербезпеки, нормативно-правового регулювання у сфері інформаційної безпеки, а також стимулювання розвитку національних технологій, здатних зменшити залежність від зовнішніх ринків.

Для ефективної реалізації інноваційно-інвестиційних стратегій доцільно зосередити увагу на таких напрямах (рисунок 1).

Рисунок 1. Механізми вдосконалення стратегування інноваційно-інвестиційного потенціалу

Джерело: складено авторами на основі О. Гуцалюк *та ін*. (2023); В. Геєць (2007); О. Якушев (2014).

Звідси випливає, що трансформаційні процеси в інформаційній економіці зумовлюють необхідність переосмислення стратегічних підходів до формування інноваційно-інвестиційного потенціалу. Для України це завдання є особливо актуальним у зв'язку з потребою забезпечення економічної стійкості та захисту національних інтересів.

Ефективне стратегування має ґрунтуватися на синергії інноваційного розвитку, інвестиційної активності та інформаційної безпеки. Поєднання економічних і безпекових компонентів у єдиній стратегії дозволить не лише зміцнити конкурентоспроможність національної економіки, але й створити умови для її сталого розвитку в умовах глобальних інформаційних змін.

У сучасних умовах глобальної цифровізації інформаційно-комунікаційні технології (ІКТ), штучний інтелект (ШІ), великі дані, блокчейн та суміжні інновації стають ключовими драйверами трансформації економіки та суспільства. Їх використання безпосередньо впливає на забезпечення національної безпеки, ефективність державного управління, розвиток фінансових систем і зростання конкурентоспроможності країни.

З метою систематизації основних напрямів впливу цих технологій на державну політику та стратегічні інтереси країни сформовано таблицю 1.

Таблиця 1. Роль ІКТ, ШІ, великих даних, блокчейну та суміжних інновацій у зміцненні стратегічних інтересів держави

Вектори впливу	Технологічні інструменти	Приклади й ефекти
1. Ситуаційна обізнаність і раннє попередження	Сенсори, супутники, OSINT, кібермоніторинг, аналітика в реальному часі	Контрзаходи AI-загрозам, адаптивний захист критичної інфраструктури (TechRadar)
2. Економічна стійкість і зростання	Прозорі фінанси, податкова аналітика, smart-регулювання, R&D-кластери	Інтеграція Digital Europe Programme і Horizon Europe для інноваційного розвитку
3. Безпека і суверенітет даних	Кібербезпека, локалізація даних, криптозахист	AI у забезпеченні кіберстійкості критичної інфраструктури (WIRED)
4. Інформаційна резильєнтність	Інструменти боротьби з дезінформацією, медіаграмотність, DLT	Використання blockchain для перевірки аутентичності інформації (arXiv)
5. Довіра і легітимність	Прозорі реєстри, відкриті дані, е-сервіси	Естонський досвід цифрового урядування, блокчейн-реєстри (WIRED, ResearchGate)
6. Міжнародна інтеграція	Стандарти ISO/NIST, дата-простори, транскордонні сервіси	Координація глобальних стандартів і цифрових мереж (Agency of European Innovations)

Джерело: сформовано авторами на основі S. Antani (2025), В. Міщенко (2024), О. Филипенко та Г. Синицина (2023), G. Graff (2024), P. Fraga-Lamas та M. Tiago (2020), O. Havryliuk *та ін*. (2023)

Таким чином, цифрові технології працюють як мультиплікатор державної спроможності: дають швидку обізнаність, прозорість, керованість ризиками й довіру. Критично важливо будувати це на єдиній архітектурі даних, сильній кібербезпеці, етичних рамках ШІ та інститутах, здатних масштабувати інновації без втрати прав людини й суверенітету.

В умовах цифрової трансформації безпека держави дедалі більше залежить від стійкості її інформаційного простору, критичної інфраструктури та систем управління даними. Швидкий розвиток технологій, зокрема штучного інтелекту, хмарних рішень та автоматизованих систем, відкриває нові можливості для економічного зростання та інновацій, але водночас породжує низку загроз. Кібератаки, техногенні збої, витоки даних і гібридні сценарії стають не лише викликом для державних структур, а й серйозним фактором ризику для національної безпеки загалом.

У цьому контексті важливо окреслити ключові вектори ризиків, які потребують системного моніторингу, швидкого реагування та розвитку комплексної стратегії кіберзахисту. Вони охоплюють три критичні сфери: кібербезпеку, захист критичної інфраструктури та суверенітет даних.

Разом із цим подолання викликів можливе лише за умови інтеграції державних, приватних та наукових ініціатив, формування культури кіберграмотності й розвитку міжнародного партнерства у сфері цифрової безпеки. Саме на цих засадах базується подальший аналіз ризиків і перспектив протидії загрозам (таблиця 2).

Таблиця 2. Ключові ризики та загрози цифровізації

Сфера ризиків	Конкретні прояви	Детальний опис та наслідки
Кібербезпека	Кібератаки на державні та приватні системи	Зростає кількість DDoS-атак, фішингових кампаній і шкідливого ПЗ. Метою стають державні органи, фінансові установи та критична інфраструктура, що може паралізувати їхню роботу.
	Атаки на ланцюги постачання (supply chain attacks)	Компрометація ПЗ чи обладнання на етапі розробки/доставки створює «бекдори» у державних системах, що відкриває шлях до масштабного несанкціонованого доступу.
	Низький рівень кіберграмотності персоналу	Людський фактор залишається головним вектором атак. Соціальна інженерія, фішинг і невміння розпізнавати загрози сприяють успішності атак.
	Використання ШІ у кіберзлочинності	Автоматизація атак, створення переконливих фішингових листів і deepfake-контенту для дискредитації держави та підриву довіри громадян.
	Недостатня швидкість реагування	CERT/CSIRT мають обмежені ресурси. Відсутність оперативної координації під час масових атак підвищує масштаб шкоди.
Захист критичної інфраструктури	Залежність від цифрових технологій	Автоматизація енергетики, транспорту, фінансів створює «єдині точки відмови». Атака або збій здатні паралізувати цілі сектори.
	Кіберфізичні загрози	SCADA/ICS-системи уразливі для атак. Можливі відключення електроенергії, аварії в логістиці та водопостачанні.
	Вразливість старих систем	Застаріле обладнання й ПЗ не мають сучасних механізмів захисту, стаючи «слабкою ланкою» інфраструктури.
	Гібридні загрози	Поєднання кібератак із фізичними диверсіями та дезінформаційними кампаніями підсилює загальний вплив на державу.
	Висока інтегрованість секторів	Взаємозалежність (енергетика ↔ транспорт ↔ телекомунікації) створює ефект «ланцюгової реакції», де збій в одному секторі провокує колапс інших.
Суверенітет даних	Залежність від іноземних хмарних сервісів	Зберігання даних за кордоном створює ризики недоступності у кризових умовах та підвищує залежність від іноземних провайдерів.
	Правові колізії	Юрисдикційні конфлікти: іноземні держави можуть вимагати доступ до персональних чи державних даних. Це знижує національний контроль.
	Неконтрольований витік даних	Недостатній контроль за доступом до даних створює загрозу шпигунства, маніпуляцій і дискредитації уряду.
	Монополізація даних корпораціями	Концентрація інформації у глобальних IT-гігантах підриває суверенітет і обмежує можливості держави контролювати дані.
	Квантова загроза	У майбутньому квантові комп'ютери можуть зламати сучасні криптоалгоритми, що поставить під загрозу безпеку комунікацій і захист державних секретів.

Джерело: сформовано авторами Defending Against Software Supply Chain Attacks (2021), K. Larsen (2025)

Цифровізація відкриває значні можливості для підвищення ефективності державного управління, економічного розвитку та зміцнення стратегічних інтересів держави. Водночас вона породжує нові ризики, серед яких найбільш критичними для національної безпеки є

зростаюча складність і масштаб кібератак, вразливість критичної інфраструктури до кіберфізичних впливів, а також ризики втрати контролю над стратегічно важливими даними.

Мінімізація цих загроз потребує комплексного підходу: інтегрованої політики кіберстійкості, розвитку національних дата-центрів та хмарних інфраструктур, переходу на постквантову криптографію, а також створення координаційних інституцій для управління ризиками цифрової трансформації. Такий підхід дозволяє забезпечити баланс між використанням інноваційних технологій та захистом національних інтересів.

Модель «Цифрова держава 3D: Data–Defense–Development» відображає багаторівневу структуру цифрового державного управління, де ключові технології, сервіси та аналітика інтегруються для забезпечення безпеки, суверенітету та розвитку економіки. Вона демонструє логіку побудови цифрової держави через шари: від базових основ безпеки до інтегрованих екосистем GovTech/DefenseTech, при цьому враховуючи поперечні шари управління, стандартизації, етики та кадрового розвитку (таблиця 3).

Таблиця 3. Концептуальна модель «Цифрова держава 3D»: Data–Defense–Development

Рівень / Компонент	Фокус	Приклади / Технології	Примітки / Поперечні шари
ОСНОВИ БЕЗПЕКИ ТА СУВЕРЕНІТЕТУ (Defense)	Захист даних та систем	Zero Trust, криптографія (зокрема постквантова), SOC/CERT, резервування, DLP	AI & Data Ethics, Privacy-by-design, ERM, кадровий капітал
ІНФРАСТРУКТУРА (Defense)	Технічне забезпечення цифрової держави	Держхмара + сертифіковані мультихмари, edge/IoT, мережі зв'язку	Управління, стандартизація, кіберстійкість
ДАНІ ТА ІНТЕГРАЦІЯ (Data)	Централізація та стандартизація даних	Дата-фабрика/лейк, каталоги, метадані, API-by-default, подієва шина	Governance, стандарти ISO/NIST/ETSI, ERM, приватність
АНАЛІТИКА, ШІ, МОДЕЛЮВАННЯ (Data)	Прийняття рішень на основі даних	Big Data, MLOps/ModelOps, цифрові двійники, симуляції політик	Використання етичних рамок AI & Data Ethics та інтероперабельності
ДЕРЖСЕРВІСИ ТА СЕКТОРИ (Development)	Цифрове урядування та публічні послуги	е-ідентичність, е-послуги, критична інфраструктура, фінанси, охорона здоров'я, освіта	Етичні та правові стандарти, управління та Privacy-by-design
ЕКОСИСТЕМА ТА РИНКИ (Development)	Розвиток інновацій та економіки	GovTech/DefenseTech, кластери, державно-приватне партнерство (ППП), експорт IT	Інтегрується з управлінням ризиками, стандартами і кадровим капіталом

Джерело: сформовано авторами

Отже, модель «Цифрова держава 3D» демонструє інтеграцію трьох ключових вимірів: Data–Defense–Development, де дані та аналітика формують основу для стратегічних рішень, безпека і суверенітет забезпечують стійкість держави, а розвиток і цифрові сервіси стимулюють економічне зростання та ефективність управління.

Поперечні шари – управління, право та етика, стандарти, управління ризиками, приватність і кадровий капітал – забезпечують координацію та збалансованість усіх рівнів моделі. Такий підхід дозволяє державі одночасно захищати національні інтереси, ефективно інтегрувати інноваційні технології та створювати стійкі цифрові сервіси для громадян і бізнесу.

Модель «Цифрова держава 3D» та її цільові групи відіграють велике значення для інтеграції даних та аналітики для стратегічних рішень – вона забезпечує централізацію даних (Data) та їх інтеграцію через державні дата-фабрики, каталоги, API-шини та подієві платформи. Це дозволяє урядовцям, аналітичним центрам, інвестиційним агентствам та органам стратегічного планування оперативно реагувати на економічні, соціальні та інфраструктурні виклики, прогнозувати ризики та приймати інноваційно орієнтовані інвестиційні рішення:

захист національних інтересів і кіберстійкість, зокрема впровадження рівня Defense із Zero Trust, постквантовою криптографією, SOC/CERT та резервуванням даних забезпечує суверенітет інформації та стійкість критичної інфраструктури. Це критично для органів

національної безпеки, правоохоронних структур, операторів критичної інфраструктури та IT-вендорів державного сектору, що відповідають за безпеку та захист стратегічних даних;

розвиток економіки та інноваційної екосистеми, адже саме рівні Development (держсервіси, GovTech/DefenseTech, кластери, державно-приватне партнерство) створюють умови для ефективного використання цифрових технологій у бізнесі та державному секторі. Це важливо для інвесторів, стартапів, R&D-підрозділів, кластерів технологічного розвитку та міжнародних партнерів, які сприяють інноваційному зростанню та конкурентоспроможності економіки;

системний та міжвідомчий підхід. Поперечні шари (управління, етика, стандарти, управління ризиками, приватність, кадровий капітал) забезпечують взаємодію всіх компонентів держави. Це є ключовим для державних органів, регуляторів, правових радників та керівників проєктів цифровізації, що координують політики, нормативні рамки та інноваційні механізми на національному рівні;

сприяння трансформаційним процесам – модель є інструментом стратегування інноваційно-інвестиційного потенціалу. Вона формує гнучку, адаптивну та прогнозовану державну систему, яка дозволяє стратегам, економістам, планувальникам інвестицій та урядовим експертам синхронізувати цифрові зміни, розвиток технологій та економічні процеси з метою захисту національних інтересів.

Інноваційно-інвестиційна політика держави в контексті моделі «Цифрова держава 3D» виступає практичним інструментом реалізації інноваційно-інвестиційної політики, оскільки дозволяє синхронізувати цифровізацію, розвиток технологій та економічні процеси, зберігаючи при цьому національні інтереси та стратегічну автономію.

Інноваційно-інвестиційна політика та рівень Data – централізація та інтеграція даних через державні дата-фабрики, каталоги, API-шини та подієві платформи – створює основу для стратегічного прийняття рішень. Держава може прогнозувати економічні та соціальні ризики, визначати перспективні інвестиційні напрями, сприяти розвитку високотехнологічних секторів та інноваційних стартапів, одночасно забезпечуючи прозорість і контроль за інвестиційними потоками.

Механізми регулювання та рівень Defense – впровадження кіберстійких рішень, постквантової криптографії, SOC/CERT та резервування даних – дозволяє державі контролювати ризики при залученні інвестицій, захищати критичну інфраструктуру та стратегічні галузі. Регуляторні «пісочниці», стандартизація та аудит технологій забезпечують баланс між відкритістю ринку для інвесторів і захистом національних інтересів.

Сприятливе середовище для інновацій та рівень Development – розвиток держсервісів, GovTech/DefenseTech, кластерів і державно-приватного партнерства – створює умови для ефективного використання цифрових технологій у бізнесі та державному секторі. Це стимулює інвестиції у R&D, міжнародну інтеграцію та комерціалізацію інноваційних проєктів, забезпечуючи зростання економіки та конкурентоспроможність держави.

Баланс між відкритістю економіки та захистом національних інтересів – відкритість економіки для іноземних інвестицій і технологій поєднується із захистом критичних даних, інфраструктури та технологічної автономії – досягається завдяки міжвідомчій координації, інтеграції поперечних шарів моделі (управління, етика, стандарти, управління ризиками, кадровий капітал), що забезпечує стійкість і прогнозованість економічного розвитку.

Застосування моделі «Цифрова держава 3D» у контексті інноваційно-інвестиційної політики дозволяє перетворити трансформаційні процеси на стратегічний інструмент розвитку економіки, де цифровізація, кіберстійкість і стимулювання інновацій взаємопов’язані, а національні інтереси та безпека держави залишаються пріоритетом.

Трансформаційні процеси у стратегуванні інноваційно-інвестиційного потенціалу національної економіки стають все тісніше пов’язаними з цифровими змінами та розвитком технологічної інфраструктури. Впровадження моделей, таких як «Цифрова держава 3D:

Data–Defense–Development», демонструє необхідність комплексного підходу, що поєднує управління даними, кіберстійкість та розвиток інноваційної екосистеми.

Цифровізація дозволяє оперативно інтегрувати дані, прогнозувати ризики, приймати стратегічно важливі інвестиційні рішення і підвищувати ефективність державного управління. Водночас вона підвищує вразливість критичних секторів, що потребує розвитку кіберзахисту, постквантової криптографії та координаційних механізмів для управління ризиками.

Модель «Цифрова держава 3D» забезпечує синергію між державними сервісами, інноваційними технологіями та економічними процесами, створюючи умови для розвитку R&D, державно-приватного партнерства та міжнародної інтеграції. Поперечні шари, включно з управлінням, етикою, стандартами, управлінням ризиками, приватністю та розвитком кадрового капіталу, дозволяють координувати інноваційні трансформації та мінімізувати загрози цифрової ери.

Таким чином, стратегування інноваційно-інвестиційного потенціалу у цифровому вимірі стає не лише інструментом економічного зростання, а й механізмом захисту національних інтересів, підвищення стійкості та конкурентоспроможності держави в умовах швидких інформаційних змін.

Висновки

Дослідження щодо трансформаційних процесів у стратегуванні інноваційно-інвестиційного потенціалу національної економіки перебувають на перетині технологічних, економічних та інформаційних змін, що визначають сучасний розвиток держави. Інтеграція цифрових технологій, штучного інтелекту, великих даних, блокчейн-рішень та суміжних інновацій формує умови для підвищення ефективності управління державними ресурсами, прогнозування економічних ризиків та прийняття стратегічно орієнтованих інвестиційних рішень.

Слід зазначити, що розбудова моделі «Цифрова держава 3D: Data–Defense–Development» демонструє практичну необхідність комплексного підходу: Data забезпечує централізацію та інтеграцію даних для аналітики, планування та контролю інвестицій; Defense гарантує кіберстійкість, захист критичної інфраструктури та стратегічних даних; Development стимулює розвиток держсервісів, інноваційних кластерів, публічно-приватних партнерств та високотехнологічного бізнесу.

Інноваційно-інвестиційна політика держави, спрямована на високотехнологічні сектори, має враховувати баланс між економічною відкритістю та захистом національних інтересів. Розвиток сприятливого середовища для інвестицій, використання регуляторних механізмів і цифрових інструментів дозволяють зменшити ризики втрати контролю над стратегічними ресурсами і забезпечити конкурентоспроможність національної економіки.

Поперечні шари моделі – управління, етика, стандарти, управління ризиками, приватність та кадровий капітал – забезпечують міжвідомчу координацію, прогнозованість трансформацій і стійкість державної системи до зовнішніх та внутрішніх викликів.

Таким чином, стратегування інноваційно-інвестиційного потенціалу у сучасних умовах інформаційних змін перетворюється на інтегрований процес, який поєднує цифрову трансформацію, розвиток технологічної інфраструктури та захист національних інтересів. Реалізація цієї моделі дозволяє державі формувати гнучку, адаптивну та конкурентоспроможну економіку, здатну швидко реагувати на виклики глобальної та національної безпеки, а також забезпечувати довгострокове сталий розвиток країни.

Подяки

Немає.

Конфлікт інтересів

Немає.

Список використаних джерел

Гальчинський, О. (2023). Інформаційна безпека як складова національної безпеки. *Інвестиції: практика та досвід, 18*. doi: 10.32702/2306-6814.2023.18.229

Геєць, В. М. (2007). *Стратегічні виклики XXI століття суспільству та економіці України. Інноваційно-технологічний розвиток економіки*. Київ : Фенікс. Т. 2.

Гуцалюк, О. М., & Бондар, Ю. А. (2023а). Взаємодія фінансового та реального секторів економіки. *Проблеми та перспективи розвитку фінансової системи в сучасних умовах*: зб. матеріалів IV Міжнар. наук.-практ. інтернет-конф. (с. 113–117) (м. Полтава, 20–21 квіт. 2023 р.). Полтава : ПУЕТ.

Гуцалюк, О. М., & Бондар, Ю. А. (2023б). Процеси цифровізації України на шляху до ЄС. *Європейський союз і Україна: передісторія, історія, сучасність*: тези Міжнар. наук. конф. (с. 27–30) (м. Миколаїв, 16 черв. 2023 р). Миколаїв : Чорноморський нац. ун-т імені Петра Могили.

Гуцалюк, О. М., Бондар, Ю. А., & Зайченко, В. В. (2025а). Організаційні імперативи формування економічної безпеки корпоративно-інтегрованих підприємств та об'єднань в індустрії гостинності. *Стратегія відновлення деокупованих територій України: виклики постконфліктного розвитку та шляхи їх подолання* : кол. монографія (с. 566–581). Івано-Франківськ : ХДУ.

Гуцалюк, О. М., Бондар, Ю. А., Журило, І. В., & Соколенко, А. В. (2025б). Стратегічний розвиток підприємств малого та середнього бізнесу в системі інноваційно-інтегрованих кластерних структур. *Економічний вісник Донбасу, 1*(79), 77–85. doi: 10.12958/1817-3772-2025-1(79)-77-85

Жаліло, Я. А. (2009). *Теорія та практика формування ефективної економічної стратегії держави*: монографія. Київ : НІСД.

Зянько, В. В., & Єпіфанова, І. Ю. (2015). *Інноваційна діяльність підприємств та її фінансове забезпечення в умовах трансформаційних змін економіки України*: монографія. Вінниця : ВНТУ.

Кравченко, В. І. (2016). Виклики і загрози Україні, її економіці та фінансам у першій третині XXI століття. *Ефективна економіка, 10*. Взято з http://www.economy.nayka.com.ua

Міщенко, В. (2024). Механізми регулювання процесів цифровізації для забезпечення національно укоріненої стійкості економічного розвитку. *Економічний простір, 189*, 283–290. doi: 10.32782/2224-6282/189-50

Филипенко, О., & Синицина, Г. (2023). Основні тренди та перспективи цифровізації економіки України. *Бізнес Інформ, 3*, 43–50. doi: 10.32983/2222-4459-2023-3-43-50

Якушев, О. (2014). Світовий досвід розвитку кластерів: можливості адаптації в Україні. *Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки*, *1*(38).

Якушев, О. В., & Якушева, О. В. (2018). Управління бізнес-процесами регіону на засадах впровадження інноваційно-освітніх кластерів. *Соціально-економічний розвиток регіонів в контексті міжнародної інтеграції, 28*(17), 65–70.

Antani, S. (2025). AI-powered cyberattacks have devastating potential – but governments can fight fire with fire. Retrieved from https://www.techradar.com/pro/ai-powered-cyberattacks-have-devastating-potential-but-governments-can-fight-fire-with-fire?utm_source

Castells, M. (2010). *The Information Age: Economy, Society and Culture*. Wiley Blackwell.

Defending against software supply chain attacks. (2021). Retrieved from https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf

Fraga-Lamas, P., & Tiago, M. (2020). Fernández-Caramés fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. *IT Professional*, *2*(22). doi: 10.48550/arXiv.1904.05386

Graff, G. M. (2024). A top White House cyber official sees the 'Promise and peril' in AI. Retrieved from https://www.wired.com/story/anne-neuberger-cybersecurity-q-and-a/?utm_source

Havryliuk, O., Yakushev, O., Petchenko, M., Zachosova, N., Bielialov, T., & Kozlovska, S. (2023). Cyber security and artificial intelligence in the context of ensuring business security in wartime. *Financial and credit activity problems of theory and practice*, *6*(53), 451–459. doi: 10.55643/fcaptp.6.53.2023.4130

Kopp, C. M. (2023). Creative destruction: Out with the old, in with the new. Retrieved from https://www.investopedia.com/terms/c/creativedestruction.asp?utm_source

Larsen, K. (2025). Europe's data sovereignty challenge. Retrieved from https://www.keepit.com/blog/data-sovereignty-europe/?utm_source

Schumpeter, J. (1942). *Capitalism, Socialism, and Democracy*. Harper & Brothers.

Yakushev, O., Moisieienko, L., Yakusheva, O., Prodanova, L., Plaksiuk, O., & Chepurda, L. (2024). Socio-economic sustainability of the tourism sector enterprises in the context of the Covid-19 pandemic: Global and Ukrainian dimensions. *Financial & Credit Activity: Problems of Theory & Practice*, *5*(58), 484–499. doi: 10.55643/fcaptp.5.58.2024.4377

Yakushev, O., Zachosova, N., Zhurba, I., Zubarieva, H., & Svishchenko, H. (2022). Personnel security management of enterprise as a component of social protection and social stability in society. *Збірник наукових праць Черкаського державного технологічного університету. Серія: Економічні науки. 65*, 4–15. doi: 10.24025/2306-4420.65.2022.262869

References

Antani, S. (2025). AI-powered cyberattacks have devastating potential – but governments can fight fire with fire. Retrieved from https://www.techradar.com/pro/ai-powered-cyberattacks-have-devastating-potential-but-governments-can-fight-fire-with-fire?utm_source

Castells, M. (2010). *The Information Age: Economy, Society and Culture*. Wiley Blackwell.

Defending against software supply chain attacks. (2021). Retrieved from https://www.cisa.gov/sites/default/files/publications/defending_against_software_supply_chain_attacks_508.pdf

Filipenko, O., & Synytsyna, H. (2023). Main trends and prospects for digitalization of the Ukrainian economy. *Biznes Inform, 3*, 43–50. doi: 10.32983/2222-4459-2023-3-43-50

Fraga-Lamas, P., & Tiago, M. (2020). Fernández-Caramés fake news, disinformation, and deepfakes: Leveraging distributed ledger technologies and blockchain to combat digital deception and counterfeit reality. *IT Professional, 2*(22). doi: 10.48550/arXiv.1904.05386

Graff, G. M. (2024). A top White House cyber official sees the 'Promise and peril' in AI. Retrieved from https://www.wired.com/story/anne-neuberger-cybersecurity-q-and-a/?utm_source

Halchynskyi, O. (2023). Information security as a component of national security. *Investytsii: praktyka ta dosvid, 18*. doi: 10.32702/2306-6814.2023.18.229

Havryliuk, O., Yakushev, O., Petchenko, M., Zachosova, N., Bielialov, T., & Kozlovska, S. (2023). Cyber security and artificial intelligence in the context of ensuring business security in wartime. *Financial and credit activity problems of theory and practice*, *6*(53), 451–459. doi: 10.55643/fcaptp.6.53.2023.4130

Heiets, V. M. (2007). *Strategic challenges of the 21st century to the society and economy of Ukraine. Innovative and technological development of the economy*. Kyiv : Phoenix. Vol. 2.

Hutsaliuk, O. M., & Bondar, Yu. A. (2023a). Interaction of the financial and real sectors of the economy. *Problems and prospects for the development of the financial system in modern conditions* : collection of materials of the IV International Scientific and Practical Internet Conference (pp. 113–117) (Poltava, April 20–21, 2023). Poltava : PUET.

Hutsaliuk, O. M., & Bondar, Yu. A. (2023b). Processes of digitalization of Ukraine on the way to the EU. *The European Union and Ukraine: Prehistory, history, modernity* : theses of the International Scientific Conference (pp. 27–30) (Mykolaiv, June 16, 2023). Mykolaiv : Petro Mohyla Black Sea National University.

Hutsaliuk, O. M., Bondar, Yu. A., & Zaichenko, V. V. (2025a). Organizational imperatives of forming economic security of corporate-integrated enterprises and associations in the hospitality industry. *Strategy for the restoration of deoccupied territories of Ukraine: Challenges of post-conflict development and ways to overcome them* : col. monograph (pp. 566–581). Ivano-Frankivsk : KhDU.

Hutsaliuuk, O. M., Bondar, Yu. A., Zhurylo, I. V., & Sokolenko, A. V. (2025b). Strategic development of small and medium-sized businesses in the system of innovative and integrated cluster structures. *Ekonomichnyi visnyk Donbasu*, *1*(79), 77–85. doi: 10.12958/1817-3772-2025-1(79)-77-85

Kopp, C. M. (2023). Creative destruction: Out with the old, in with the new. Retrieved from https://www.investopedia.com/terms/c/creativedestruction.asp?utm_source

Kravchenko, V. I. (2016). Challenges and threats to Ukraine, its economy and finance in the first third of the XXI century. *Efektyvna ekonomika, 10*. Retrieved from http://www.economy.nayka.com.ua

Larsen, K. (2025). Europe's data sovereignty challenge. Retrieved from https://www.keepit.com/blog/data-sovereignty-europe/?utm_source

Mishchenko, V. (2024). Mechanisms for regulating digitalization processes to ensure nationally rooted sustainability of economic development. *Ekonomichnyi prostir, 189*, 283–290. doi: 10.32782/2224-6282/189-50

Schumpeter, J. (1942). *Capitalism, Socialism, and Democracy*. Harper & Brothers.

Yakushev, O. (2014). World experience in cluster development: Possibilities for adaptation in Ukraine. *Collection of scientific papers of Cherkasy State Technological University. Series: Economic Sciences, 1*(38).

Yakushev, O. V., & Yakusheva, O. V. (2018). Management of regional business processes based on the implementation of innovation and educational clusters. *Sotsialno-ekonomichnyi rozvytok rehioniv v konteksti mizhnarodnoi intehratsii, 28*(17), 65–70.

Yakushev, O., Moisieienko, L., Yakusheva, O., Prodanova, L., Plaksiuk, O., & Chepurda, L. (2024). Socio-economic sustainability of the tourism sector enterprises in the context of the Covid-19 pandemic: Global and Ukrainian dimensions. *Financial & Credit Activity: Problems of Theory & Practice, 5*(58), 484–499. doi: 10.55643/fcaptp.5.58.2024.4377

Yakushev, O., Zachosova, N., Zhurba, I., Zubarieva, H., & Svishchenko, H. (2022). Personnel security management of enterprise as a component of social protection and social stability in society. *Collection of scientific papers of Cherkasy State Technological University. Series: Economic Sciences*. *65*, 4–15. doi: 10.24025/2306-4420.65.2022.262869

Zhalilo, Ya. A. (2009). *Theory and practice of forming an effective economic strategy of the state* : monograph. Kyiv : NISD.

Zianko, V. V., & Yepifanova, I. Yu. (2015). *Innovative activity of enterprises and its financial support in the conditions of transformational changes in the economy of Ukraine* : monograph. Vinnytsia : VNTU.