

БЕЗПЕКОВИЙ ВИМІР ДОМІНАНТНИХ ТЕНДЕНЦІЙ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ ЕКОНОМІКИ¹

Маслій Олександра Анатоліївна*, кандидат економічних наук, доцент,
доцент кафедри фінансів, банківського бізнесу та оподаткування
Науменко Олександр Андрійович**, здобувач третього (наукового) рівня вищої освіти
Національний університет «Полтавська політехніка
імені Юрія Кондратюка»

*ORCID 0000-0003-2184-968X

**ORCID 0009-0006-9943-9460

Дата надходження статті: 25.03.2026

Дата прийняття статті: 15.04.2026

Дата публікації статті: 29.05.2026

Вступ. Впровадження інформаційно-комунікаційних технологій у всіх сферах соціально-економічної діяльності докорінно трансформує механізми створення доданої вартості, актуалізує безпековий вимір цифрового розвитку й зумовлює якісне переосмислення змісту економічної безпеки держави. Цифровізація економіки, для якої характерне впровадження новітніх технологій (аналізу великих даних, Інтернету речей, штучного інтелекту, хмарних обчислень), що стимулюють економічне зростання, супроводжується формуванням нових системних ризиків, пов'язаних із кіберзагрозами критичній інфраструктурі, поглибленням цифрової нерівності, монополізації цифрових платформ, зростаючої технологічної залежності тощо [1]. Розгляд безпекового виміру основних тенденцій цифрової трансформації економіки набуває особливої актуальності в контексті забезпечення стійкості та здатності національної економічної системи до саморозвитку в умовах цифровізації. З огляду на масштабність трансформаційних змін в економіці виникає необхідність у перегляді парадигми економічної безпеки держави та особливостей забезпечення незалежності, стійкості та здатності цифрової економіки до саморозвитку і прогресу з урахуванням домінантного впливу цифрових ризиків і загроз.

Огляд останніх джерел досліджень і публікацій. Проблематика забезпечення економічної безпеки держави в умовах цифрового переходу та формування цифрового суспільства активно досліджується у наукових працях українських та зарубіжних учених. У роботі Кириленка С. В. [2] розроблено комплексний підхід до формування системи економічної безпеки в умовах трансформаційних змін та цифрової економіки. У працях Гриценка А. А., Бурлай Т. В. [3], Хаустової М. Г. [4] розглядається вплив цифровізації на соціальний розвиток. Значна кількість наукових праць присвячена вивченню впливу цифровізації на певні сфери економічної діяльності. Так, Юрчук Н. П. та Кіпоренко С. С. [7] досліджують виклики і можливості для сільськогосподарських господарств під впливом цифрових технологій, а Кретов Д. Ю. та Міндова О. І. [8] вивчають перспективи розвитку банківського сектору України в умовах цифровізації. Швидка Д. Ю. та Дзюбенко Л. М. [9], у свою чергу, фокусують увагу на малому бізнесі, а саме перспективах і ризиках його розвитку в умовах цифрової трансформації. Водночас, попри наявність значної кількості наукових досліджень впливу цифровізації на окремі галузі національного господарства, виявлена фрагментарність у вивченні впливу домінантних тенденцій цифрової трансформації

¹ Виконано в рамках науково-дослідної теми «Розробка стратегії цифрового майбутнього України: безпековий вимір економічного розвитку» (№ д/р 0126U000632), що фінансується за рахунок коштів державного бюджету.



на концептуальні засади економічної безпеки держави, а саме забезпечення незалежності, стійкості й здатності цифрової економіки до саморозвитку і прогресу.

Метою статті є аналіз домінуючих тенденцій цифрової трансформації економіки та їх впливу на формування цифрових розривів і загроз економічній безпеці держави, а також обґрунтування необхідності трансформації парадигми економічної безпеки в умовах цифровізації.

Основний матеріал і результати. Цифровізація як провідний соціально-економічний тренд сучасних суспільних трансформацій підвищує ефективність виробництва та якість життя. Основними технологічними драйверами цих змін є аналіз великих даних, інтернет речей, хмарні технології, 3D-друк та, особливо, штучний інтелект [3, 4]. Ці технології змінюють господарську діяльність, перетворюючи дані у цифровій формі на визначальний чинник економічного розвитку.

Цифрова трансформація охоплює всі сектори економіки та державне управління, фундаментально змінюючи способи ведення господарської діяльності, бізнес-моделі, операційні процеси та підходи до врядування. Впровадження сучасних цифрових трансформацій дозволяє підвищувати стійкість та гнучкість національної економіки, що є основою економічної безпеки держави [10].

З огляду на домінування аграрного сектору в експортній структурі України варто відзначити, що цифрова трансформація сільськогосподарських підприємств відіграє вагомий роль у забезпеченні економічної безпеки держави, підвищенні стійкості та результативності національної економіки через оптимізацію витрат агробізнесу, підвищення його рентабельності та продуктивності. Застосування цифрових технологій, зокрема, комплексного управління технікою, системного обліку палива, точного та розумного землеробства на основі безперервного збору і аналізу даних, сприяє підвищенню ефективності управлінських рішень та точності планування в агропромисловому комплексі (АПК). Використання дронів, датчиків, систем інтернету речей та аналізу великих даних є основою оптимізації управління ресурсами, зокрема через зменшення витрат на добрива й пестициди [7]. Таким чином, цифровізація в АПК України є важливим фактором для підвищення конкурентоспроможності національної економіки та забезпечення її сталого розвитку.

Вагоме значення для економічної безпеки держави мають процеси цифрової трансформації у банківській системі, що є основою фінансового сектору економіки України. Перегляд банківськими установами традиційних бізнес-моделей, що базуються на фізичних філіях та офісах, на користь більш гнучких та цифрових підходів, автоматизація банківських процесів, таких як кредитний скоринг та обробка документів, значно підвищує ефективність банківської діяльності й знижує операційні витрати банків. Перехід до електронного документообігу, впровадження автоматизованих процесів та використання банками чат-ботів на основі штучного інтелекту для взаємодії з клієнтами сприяє оптимізації бізнес-процесів, прискоренню надання послуг й економії людських та фінансових ресурсів [8].

Зважаючи на переважання вкладу малого та середнього бізнесу в структуру ВВП України, цифрова трансформація саме цього сегменту національної економіки безумовно вважається драйвером економічного зростання та підвищення економічної безпеки держави [10]. Цифрові технології, включаючи хмарні послуги, аналіз великих даних, штучний інтелект та електронну комерцію, дають змогу малим підприємствам оптимізувати бізнес-процеси, розширити ринки збуту та знизити витрати. Онлайн-платформи та цифрові інструменти маркетингу дозволяють охопити ширшу, навіть глобальну аудиторію, тоді як автоматизація управління запасами та прогнозування попиту покращують адаптивність бізнес-моделей до ринкових змін [9]. Таким чином, цифрова трансформація сприяє підвищенню стійкості економічних суб'єктів до негативних впливів екзогенних викликів і загроз, що є фундаментальним чинником зміцнення економічної безпеки держави.

Пріоритетне значення цифрової трансформації у забезпеченні сталого економічного зростання відображається в основі низки стратегічних ініціатив державних органів України. Однією з найважливіших із них є Стратегія цифрового розвитку інновацій України до 2030 року, у якій визначено бачення України у сфері технологій та інновацій, з пріоритетом на такі галузі, як DefenseTech, MedTech, AI та Agritech [6]. Утім, як засвідчує щорічне дослідження Міністерства цифрової трансформації України, має місце нерівномірний розподіл благ від цифровізації й формування дисбалансів у цифровому розвитку регіонів (рис. 1), що визначає рівень їхньої економічної безпеки в умовах цифрової трансформації соціально-економічних відносин [11]. Так, найвищий рівень цифровізації має Львівська область (54 бали зі 100) й він перевищує рівень цифровізації Кіровоградської області (із найнижчим значенням – 15 балів зі 100) у 3,6 рази [5], що підтверджує суттєвий дисбаланс у цифровому розвитку регіонів України.

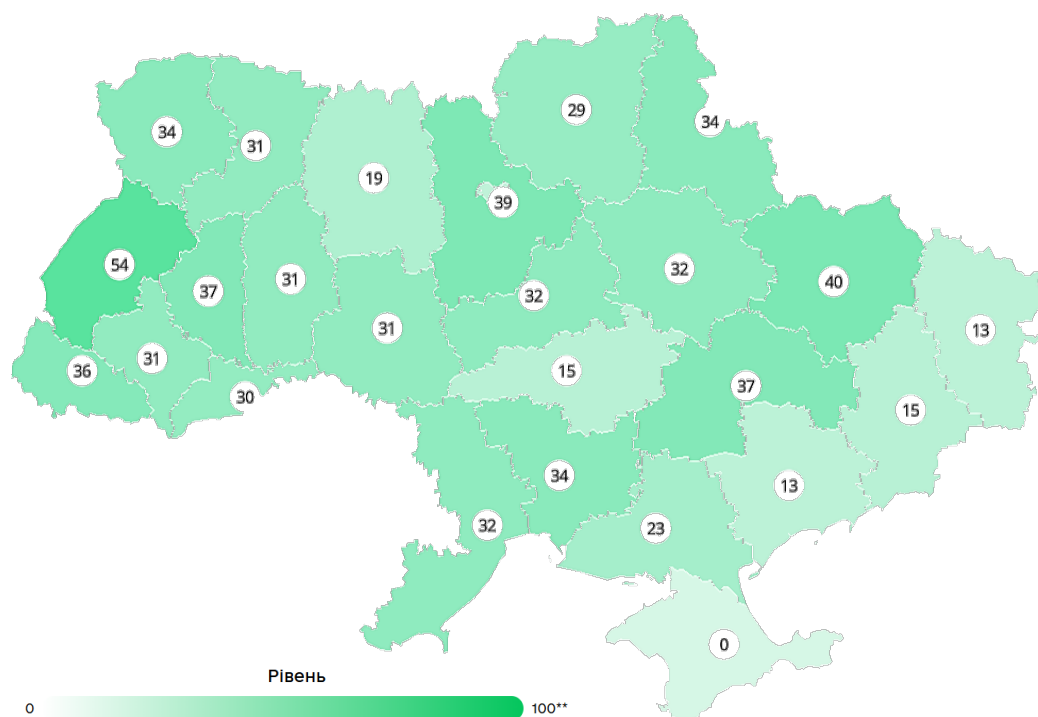


Рис. 1. Індекс цифрової трансформації територіальних громад України за регіонами у 2025 році

Джерело: за даними Міністерства цифрової трансформації України [5]

Загальносвітова статистика свідчить, що значна частина населення досі не має доступу до інтернету, що створює так звані «цифрові розриви». Дана проблема є небезпечною для країн, що розвиваються, оскільки може призвести до ще більшого відставання [6]. Для України зазначена проблема також характерна, оскільки за дослідженнями Міністерства цифрової трансформації України присутній дисбаланс у розвитку цифрової інфраструктури різних регіонів України [5].

Домінантною тенденцією цифрової трансформації на сучасному етапі розвитку беззаперечно є впровадження технологій штучного інтелекту (ШІ) в усі сфери соціально-економічних відносин. ШІ виступає одним із найбільш потужних драйверів економічного розвитку в сучасному світі, що підтверджується його глобальним використанням в усіх секторах економіки. На рівні бізнесу впровадження технологій штучного інтелекту дозволяє автоматизувати рутинні операції, що звільняє людські ресурси для виконання творчих і стратегічних завдань [12]. Застосування ШІ значно підвищує продуктивність праці та допомагає подолати дефіцит робочої сили, оскільки оптимізує використання наявних кадрів. Аналіз великих обсягів даних з використанням ШІ дозволяє приймати більш обґрунтовані та швидкі управлінські рішення, що є основним чинником підвищення конкурентоспроможності підприємств в епоху інформаційного суспільства [10].

Внесок штучного інтелекту у зростання капіталізації компаній на глобальному рівні є значним, утім, незважаючи на глобальні тенденції, в Україні цей потенціал використовується не повною мірою. Існують внутрішні бар'єри, що гальмують широке впровадження штучного інтелекту, зокрема, брак кваліфікованих спеціалістів, які могли б ефективно інтегрувати та обслуговувати ШІ-системи [13]. Керівники компаній часто демонструють консервативний підхід, побоюючись здійснювати значні інвестиції у нові технології і висловлюючи недовіру до якості результатів, що генеруються штучним інтелектом. Так, за опитуванням Торгово-промислової палати України, третина українських підприємців не використовує штучний інтелект у свої діяльності і не працює цього робити [15].

За даними опитування [15], лише 37% українських підприємств використовують штучний інтелект, тоді як 33% не застосовують його і не планують впроваджувати, 23% перебувають на етапі розгляду такої можливості, і лише 7% планують впровадження протягом найближчого року. Така розбіжність між світовими технологічними трендами та станом впровадження ШІ у українському бізнес-середовищі становить суттєвий ризик технологічного відставання. Нездатність більшості українських підприємств подолати існуючі бар'єри на шляху до впровадження сучасних інформаційно-комунікаційних

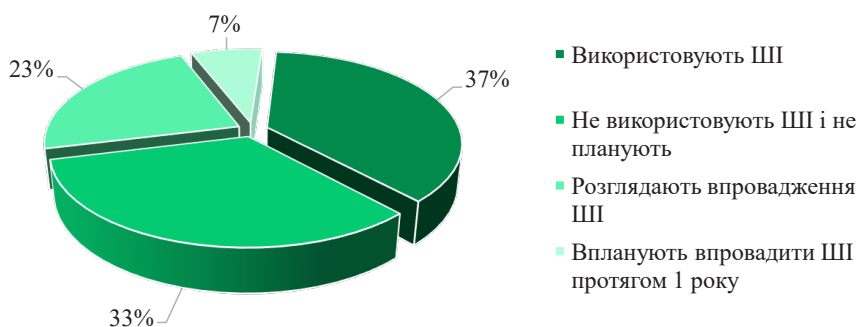


Рис. 2. Розподіл українських компаній за статусом використання ШІ станом на вересень 2025 року

Джерело: побудовано за результатами опитування Торгово-промислової палати України [15]

технологій може призвести до втрати конкурентних позицій на міжнародних ринках, що безпосередньо загрожує економічній безпеці держави.

Поряд з економічними перевагами впровадження штучного інтелекту створює додаткові виклики економічній безпеці держави, найактуальнішим із яких є ризик втрати робочих місць внаслідок автоматизації рутинних завдань (рис. 3). Хоча значна кількість робочих місць можуть бути лише частково автоматизовані, для працівників з низькою кваліфікацією зростає ризик витіснення з ринку праці, що може призвести до збільшення безробіття [14]. Цей ризик посилюється високими початковими витратами на інтеграцію ШІ-систем, які можуть бути непропорційно високими для малих та середніх підприємств України. Іншим важливим аспектом є залежність від технологій та можлива втрата навичок критичного мислення у населення через автоматизацію процесів. Крім того ШІ-системи не можуть інтерпретувати емоції, культурні особливості та етичні дилеми, що обмежує їх ефективність у сферах, де важливий людський контакт та контекст інформації [14].



Рис. 3. Переваги та ризики використання штучного інтелекту як домінантної тенденції цифрової трансформації

Джерело: сформовано на основі даних [12–14]

У науковій літературі існують суперечності та протилежні дослідження щодо впливу штучного інтелекту на зайнятість населення. Деякі науковці доводять наявність тенденцій до скорочення робочих місць внаслідок впровадження ШІ, тоді як інші дослідження підтверджують вагомість тенденції до створення нових робочих місць завдяки широкого використання ШІ, що сприяє зменшенню дефіциту робочої сили [14]. Тому реальний виклик полягає не стільки у суттєвому витісненні, скільки в трансформації ринку праці й необхідності постійного розвитку та перекваліфікації працівників у контексті адаптації до нових вимог [12]. Без системного реформування освіти та програм підвищення кваліфікації, може виникнути значний дисбаланс між попитом на ШІ-спеціалістів та надлишком некваліфікованої робочої сили. Цей дисбаланс може призвести до соціальної напруженості та зростання майнового розшарування, що є реальною загрозою економічній безпеці держави.

Іншим вагомим безпековим аспектом впливу поширення цифрових технологій на стійкість і стабільність соціально-економічної системи є розширення можливості для злочинної діяльності внаслідок перенесення значної частини господарських операцій у кіберпростір. Серед ключових цифрових загроз, що становлять ризик для економічної безпеки, науковці виділяють кібератаки, крадіжки корпоративних даних, промислове шпигунство та нові види шахрайства, зокрема з криптовалютами [16]. Пріоритетність протидії кіберзагрозам підтверджується тенденцією до зростання кількості кіберінцидентів з боку російської федерації на сайти українських компаній та урядових порталів в умовах воєнного стану (рис. 4).

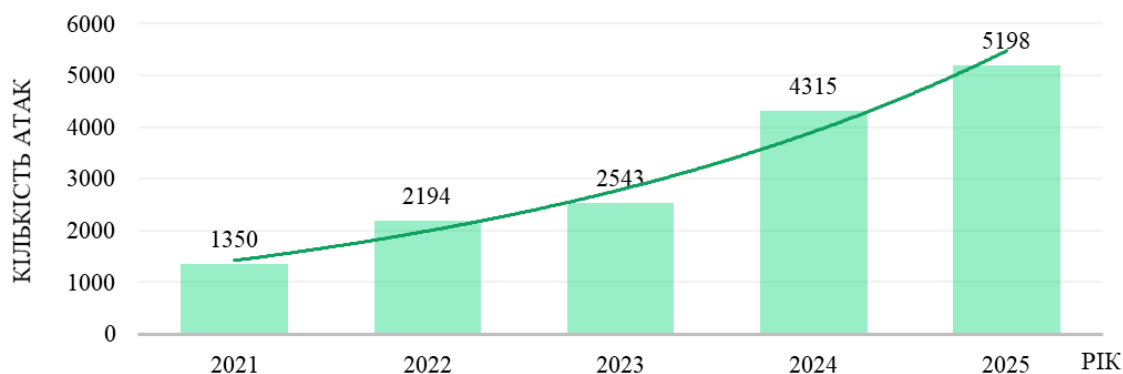


Рис. 4. Кількість кібератак на територію України у 2021–2025 роках

Джерело: побудовано авторами за даними CERT-UA [17]

Кібербезпека перетворюється у нову форму економічної конкуренції та визначальний чинник національної безпеки, адже кібератаки на критичну інфраструктуру, а саме енергетичні системи, фінансові та логістичні мережі, можуть підірвати стійкість національної економіки та становити пряму загрозу економічній безпеці держави [18]. Таким чином, інвестиції в кіберзахист варто розглядати як стратегічне вкладення у зміцнення економічної безпеки держави шляхом забезпечення стійкості інформаційної й технологічної інфраструктури держави та її економічних суб'єктів.

Трансформаційні зміни в економічній системі в результаті впровадження цифрових технологій зумовлюють зміну парадигми економічної безпеки держави й потребують перегляду стратегічних пріоритетів забезпечення стійкості національної економіки до внутрішніх і зовнішніх загроз.

Концептуальну основу економічної безпеки держави становлять економічна незалежність, стійкість, стабільність та здатність національної економіки до саморозвитку і прогресу [1], підходи до забезпечення яких мають бути адаптовані до умов цифрової економіки з урахуванням сучасних цифрових викликів, ризиків і загроз. Відповідно, для забезпечення ефективного управління економічною безпекою держави в нових умовах необхідно враховувати не лише традиційні, а й цифрові індикатори, що дозволяють отримати більш повне уявлення про стан економічної системи та її здатність протистояти цифровим викликам (табл. 1).

В умовах цифрової трансформації економічна незалежність держави виходить за межі традиційного контролю над природними й матеріальними ресурсами й першочергово визначається технологічним суверенітетом, тобто здатністю держави самостійно розробляти, виробляти та впроваджувати інноваційні технологічні рішення, уникаючи критичної залежності від імпорту технологій [18]. Висока тех-

Основні традиційні та цифрові індикатори економічної безпеки держави

Компоненти економічної безпеки держави	Традиційний індикатор	Цифровий індикатор
Економічна незалежність	Рівень ресурсної залежності економіки, баланс торгівлі	Рівень технологічного суверенітету, частка імпорту ІТ-продуктів
Стійкість та стабільність	Динаміка ВВП, рівень стабільності фінансової системи	Рівень кіберзахищеності критичної інфраструктури, кількість кіберінцидентів
Здатність до саморозвитку	Рівень інвестицій, рівень науково-технічного потенціалу	Витрати на R&D у сфері ІТ, кількість інноваційних стартапів, рівень цифрової грамотності населення

Джерело: складено автором на основі даних [2, 6]

нологічна залежність формує системну вразливість національної економіки, обмежуючи її стратегічну автономію та підриваючи фундаментальні основи економічної безпеки держави.

Стійкість економіки в сучасних умовах визначається не лише здатністю держави захищати національні економічні інтереси та пом'якшувати економічні коливання в періоди фінансових криз, а й надійністю цифрової інфраструктури як основи сталого розвитку всіх секторів економіки [17].

Здатність до саморозвитку економіки, спроможність до впровадження інновацій та прогресу на пряму залежить від швидкості впровадження сучасних цифрових технологій. Тому відставання в цифровізації стає реальною загрозою економічній безпеці держави, яка призводить до технологічного та економічного відставання держави, а в довгостроковій перспективі підриває конкурентоспроможність країни [2].

Отже, цифровізація змінює парадигму забезпечення економічної безпеки держави, виступаючи драйвером економічного розвитку та генеруючи сучасні інструменти протидії загрозам. Так, впровадження штучного інтелекту як домінуючої тенденції цифрової трансформації відіграє ключову роль у протистоянні цифровим загрозам завдяки можливості своєчасного виявлення та реагування на кібератаки шляхом обробки та аналізу великих масивів даних [10]. Технології машинного навчання дозволяють системам кібербезпеки розпізнавати закономірності та відрізняти нормальний мережевий трафік від шкідливої діяльності, що формує проактивний підхід до забезпечення економічної безпеки в умовах цифровізації. Крім того, обробка природної мови дозволяє аналітикам швидко інтерпретувати текстові дані звітів про загрози, що сприяє оперативному прийняттю рішень [12].

Утім, варто враховувати дуальний характер впливу розвитку ШІ, який будучи потужним інструментом захисту може використовуватися для створення більш складних та масованих кібератак. Хакери можуть використовувати генеративні моделі ШІ для створення переконливого фішингового контенту або для автоматизації складних атак. Такі виклики вимагають від уряду постійного нарощування спроможності та інвестування в дослідження протидії ШІ-керованим загрозам.

Висновки. Проведений аналіз домінуючих тенденцій цифровізації підтвердив складний дуальний характер їхнього впливу на економічну безпеку держави. Цифровізація як незворотний глобальний процес фундаментально трансформує суспільні відносини в усіх секторах економіки. Водночас її домінуючі тенденції генерують цифрові розриви та структурні дисбаланси у впровадженні технологій, які набувають характеру реальних додатково набутих загроз економічній безпеці держави.

За результатами систематизації переваг і ризиків використання штучного інтелекту, як основного каталізатора економічних змін на сучасному етапі цифрового розвитку, доведено необхідність зміни парадигми економічної безпеки держави та зміщення пріоритетів у бік формування технологічного суверенітету й забезпечення кіберзахищеності критичної інфраструктури як фундаментальних основ національної стійкості. Обґрунтовано доцільність доповнення чинної системи показників економічної безпеки держави цифровими індикаторами, що відкриває можливості для розроблення дієвих механізмів державної політики цифрового розвитку, які відповідають викликам сучасності.

Таким чином, забезпечення економічної безпеки держави в умовах цифрової трансформації передбачає постійне узгодження заходів стимулювання інновацій та ефективного управління ризиками. Здатність забезпечити формування адаптивної регуляторної політики, розвиток цифрових компетенцій та захист стратегічної інфраструктури визначатиме рівень економічної безпеки держави у довгостроковій перспективі.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ:

1. Маслій О.А., Кудінова А.О., Буряк А.А., Янко А.С., Білько С.С. *Детермінанти економічної безпеки держави в парадигмі цифрового розвитку*: монографія. Івано-Франківськ: НАІР, 2025. 324 с.
2. Кириленко С. В. Система економічної безпеки в умовах цифрової економіки. *Журнал стратегічних економічних досліджень*. 2024. № 1. С. 40–47. DOI: <https://doi.org/10.30857/2786-5398.2024.1.4>
3. Гриценко А., Бурлай Т. Вплив цифровізації на соціальний розвиток. *Економічна теорія*. 2020. № 3. С. 24–51. DOI: <https://doi.org/10.15407/etet2020.03.024>
4. Хаустова М. Г. Вигоди, ризики та проблеми цифровізації суспільства: загальнотеоретичний аспект. *Аналітично-порівняльне правознавство*. 2023. № 5. С. 753–759. DOI: <https://doi.org/10.24144/2788-6018.2023.05.135>
5. Індекс цифрової трансформації територіальних громад України. *Міністерство цифрової трансформації України*. URL: <https://hromada.gov.ua/index> (дата звернення: 16.03.2026)
6. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025-2027 роках: розпорядження Кабінету Міністрів України від 31.12.2024 № 1351-р. *Верховна Рада України*. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text> (дата звернення: 18.03.2026).
7. Юрчук Н. П., Кіпоренко С. С. Цифровізація сільського господарства: виклики і можливості для фермерських господарств. *Агросвіт*. 2024. № 19. С. 53–62. DOI: <https://doi.org/10.32702/2306-6792.2024.19.53>
8. Кретов Д. Ю., Міндова О. І. Цифровізація банківського сектору України: сучасний стан та перспективи розвитку. *Сталий розвиток економіки*. 2024. № 2. С. 223–228. DOI: <https://doi.org/10.32782/2308-1988/2024-49-35>
9. Швидка О. П., Дзюбенко Л. М. Інноваційні бізнес-моделі в умовах цифрової трансформації: перспективи та ризики для малого бізнесу. *Цифровізація економіки і фінансів*. 2024. № 11. С. 118–128. DOI: <https://doi.org/10.33763/finukr2024.11.117>
10. Чайкіна А., Маслій О., Черв'як А. Сучасні драйвери підвищення економічної безпеки країни в умовах цифрової трансформації. *Сталий розвиток економіки*. 2024. № 2 (49). С. 307–313. DOI: <https://doi.org/10.32782/2308-1988/2024-49-49>
11. Danylyshyn V. M., Onyshchenko S. V., Maslii O. A. Socio-economic security: modern approach to ensuring the socio-economic development of the region. *Economics and Region*, 2019. Vol. 4 (75). P. 6–13. DOI: [https://doi.org/10.26906/EiR.2019.4\(75\).1805](https://doi.org/10.26906/EiR.2019.4(75).1805)
12. Юрченко Г., Лесьо А. Роль штучного інтелекту в економічному зростанні. *Development Service Industry Management*. 2024. № 2. С. 195–200. DOI: [https://doi.org/10.31891/dsim-2024-6\(29\)](https://doi.org/10.31891/dsim-2024-6(29))
13. Білоус А. Без ШІ важко буде конкурувати. *Forbes.ua*. URL: <https://forbes.ua/company/bez-vprovadzhennya-shi-bude-skladno-konkuruvati-240-ukrainskikh-kompaniy-rozpovili-yak-voni-vikoristovuyut-shtuchniy-intelekt-analiz-trendu-vid-andriya-bilousa-27052025-30066> (дата звернення: 23.03.2026)
14. Rossomakha I., Kyrylenko O., Borysiuk A. The Impact of Artificial Intelligence on the Labor Market in the World and Particularly in Ukraine. *Economics. Finances. Law*. 2024. № 2. P. 27–30. DOI: <https://doi.org/10.37634/efp.2024.2.6>
15. 37% українських компаній вже використовують інструменти ШІ. *Торгово-промислова палата України*. URL: <https://uccr.org.ua/press-center/uccr-news/37-ukrayinskikh-kompanii-vzhe-vikoristovuyut-instrumenti-shi> (дата звернення: 23.03.2026)
16. Кудінова А.О., Маслій О.А., Буряк А.А. Формалізація ризиків і загроз економічній безпеці України в умовах цифровізації. *Управління змінами та інновації*. 2024. № 12. С. 25–31. DOI: <https://doi.org/10.32782/СМІ/2024-12-4>
17. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37%. *Державна служба спеціального зв'язку та захисту інформації України*. URL: <https://cert.gov.ua/article/17696> (дата звернення: 25.03.2026)
18. Пахненко О.М., Божко М.О. Кіберзагрози як виклик економічній безпеці: потенціал технологічної інфраструктури України. *Економіка і регіон*. 2025. № 2 (97). С. 191–197. DOI: [https://doi.org/10.26906/EiR.2025.2\(97\).3857](https://doi.org/10.26906/EiR.2025.2(97).3857)

REFERENCES:

1. Maslii O. A., Kudinova A. O., Buriak A. A., Yanko A. S., Bilko S. S. (2025) Determinanty ekonomichnoi bezpeky derzhavy v paradyhmi tsyfrovoho rozvytku: monohrafiia [Determinants of economic security of the state in the paradigm of digital development: monograph]. Ivano-Frankivsk: NAIR. (in Ukrainian)
2. Kyrylenko S. V. (2024) Systema ekonomichnoi bezpeky v umovakh tsyfrovoi ekonomiky [System of economic security in the conditions of digital economy]. Zhurnal stratehichnykh ekonomichnykh doslidzhen, no. 1, pp. 40–47. DOI: <https://doi.org/10.30857/2786-5398.2024.1.4>
3. Hrytsenko A., Burlai T. (2020) Vplyv tsyfrovizatsii na sotsialnyi rozvytok [The impact of digitalization on social development]. Ekonomichna teoriia, no. 3, pp. 24–51. DOI: <https://doi.org/10.15407/etet2020.03.024>
4. Khaustova M. H. (2023) Vyhody, ryzyky ta problemy tsyfrovizatsii suspilstva: zahalnoteoretychnyi aspekt [Benefits, risks and problems of digitalization of society: general theoretical aspect]. Analychno-porivnialne pravoznavstvo, no. 5, pp. 753–759. DOI: <https://doi.org/10.24144/2788-6018.2023.05.135>
5. Ministerstvo tsyfrovoi transformatsii Ukrainy (n.d.) Indeks tsyfrovoi transformatsii terytorialnykh hromad Ukrainy [Digital transformation index of territorial communities of Ukraine]. Available at: <https://hromada.gov.ua/index> (accessed March 16, 2026)

6. Cabinet of Ministers of Ukraine (2024) Pro skhvalennia Stratehii tsyfrovoho rozvytku innovatsiinoi diialnosti Ukrainy na period do 2030 roku ta zatverdzhennia operatsiinoho planu zakhodiv z yii realizatsii u 2025–2027 rokakh [On approval of the Strategy for digital development of innovative activity of Ukraine until 2030 and the operational plan for its implementation in 2025–2027]. Available at: <https://zakon.rada.gov.ua/laws/show/1351-2024-%D1%80#Text> (accessed March 18, 2026)
7. Yurchuk N. P., Kiporenko S. S. (2024) Tsyfrovizatsiia silskoho hospodarstva: vyklyky i mozhlyvosti dlia fermerskykh hospodarstv [Digitalization of agriculture: challenges and opportunities for farms]. *Ahrosvit*, no. 19, pp. 53–62. DOI: <https://doi.org/10.32702/2306-6792.2024.19.53>
8. Kretov D. Yu., Mindova O. I. (2024) Tsyfrovizatsiia bankivskoho sektoru Ukrainy: suchasnyi stan ta perspektyvy rozvytku [Digitalization of the banking sector of Ukraine: current state and development prospects]. *Stalyi rozvytok ekonomiky*, no. 2, pp. 223–228. DOI: <https://doi.org/10.32782/2308-1988/2024-49-35>
9. Shvydka O. P., Dziubenko L. M. (2024) Innovatsiini biznes-modeli v umovakh tsyfrovoy transformatsii: perspektyvy ta ryzyky dlia maloho biznesu [Innovative business models in the conditions of digital transformation: prospects and risks for small business]. *Tsyfrovizatsiia ekonomiky i finansiv*, no. 11, pp. 118–128. DOI: <https://doi.org/10.33763/finukr2024.11.117>
10. Chaikina A., Maslii O., Cherviak A. (2024) Suchasni draivery pidvyshchennia ekonomichnoi bezpeky krainy v umovakh tsyfrovoy transformatsii [Modern drivers of increasing the economic security of the country in the conditions of digital transformation]. *Stalyi rozvytok ekonomiky*, no. 2 (49), pp. 307–313. DOI: <https://doi.org/10.32782/2308-1988/2024-49-49>
11. Danylyshyn B. M., Onyshchenko S. V., Maslii O. A. (2019) Socio-economic security: modern approach to ensuring the socio-economic development of the region. *Economics and Region*, vol. 4 (75), pp. 6–13. DOI: [https://doi.org/10.26906/EiR.2019.4\(75\).1805](https://doi.org/10.26906/EiR.2019.4(75).1805)
12. Yurchenko H., Lieso A. (2024) Rol shtuchoho intelektu v ekonomichnomu zrostanni [The role of artificial intelligence in economic growth]. *Development Service Industry Management*, no. 2, pp. 195–200. DOI: [https://doi.org/10.31891/dsim-2024-6\(29\)](https://doi.org/10.31891/dsim-2024-6(29))
13. Bilous A. (2025) Bez ShI vazhko bude konkuruvaty [It will be difficult to compete without AI]. *Forbes.ua*. Available at: <https://forbes.ua/company/bez-vprovadzhennya-shi-bude-skladno-konkuruvati-240-ukrainskikh-kompaniy-rozpovili-yak-voni-vikoristovuyut-shtuchniy-intelekt-analiz-trendu-vid-andriya-bilousa-27052025-30066> (accessed March 23, 2026)
14. Rossomakha I., Kyrylenko O., Borysiuk A. (2024) The Impact of Artificial Intelligence on the Labor Market in the World and Particularly in Ukraine. *Economics. Finances. Law*, no. 2, pp. 27–30. DOI: <https://doi.org/10.37634/efp.2024.2.6>
15. Ukrainian Chamber of Commerce and Industry (n.d.) 37% ukrainskykh kompanii vzhe vykorystovuyut instrumenty ShI [37% of Ukrainian companies already use AI tools]. Available at: <https://ucco.org.ua/press-center/ucco-news/37-ukrayinskikh-kompanii-vzhe-vikoristovuyut-instrumenti-shi> (accessed March 23, 2026)
16. Kudinova A. O., Maslii O. A., Buriak A. A. (2024) Formalizatsiia ryzykiv i zahroz ekonomichnii bezpetsi Ukrainy v umovakh tsyfrovizatsii [Formalization of risks and threats to the economic security of Ukraine in the conditions of digitalization]. *Upravlinnia zminamy ta innovatsii*, no. 12, pp. 25–31. DOI: <https://doi.org/10.32782/CMI/2024-12-4>
17. State Service of Special Communications and Information Protection of Ukraine (2026) CERT-UA u 2025 rotsi opratsiuvala maizhe 6000 kiberintsydentiv: kilnist vorozhykh atak zrosla na 37% [CERT-UA processed nearly 6000 cyber incidents in 2025: the number of hostile attacks increased by 37%]. Available at: <https://cert.gov.ua/article/17696> (accessed March 25, 2026)
18. Pakhnenko O. M., Bozhko M. O. (2025) Kiberzahrozy yak vyklyk ekonomichnii bezpetsi: potentsial tekhnolohichnoi infrastruktury Ukrainy [Cyber threats as a challenge to economic security: the potential of Ukraine's technological infrastructure]. *Ekonomika i rehion*, no. 2 (97), pp. 191–197. DOI: [https://doi.org/10.26906/EiR.2025.2\(97\).3857](https://doi.org/10.26906/EiR.2025.2(97).3857)

УДК 338.2:004.9:338.1

JEL F52, O33, O38

Маслій Олександра Анатоліївна, кандидат економічних наук, доцент, доцент кафедри фінансів, банківського бізнесу та оподаткування, Національний університет «Полтавська політехніка імені Юрія Кондратюка». **Науменко Олександр Андрійович**, здобувач третього (наукового) рівня вищої освіти, Національний університет «Полтавська політехніка імені Юрія Кондратюка». **Безпековий вимір домінантних тенденцій цифрової трансформації економіки.**

У статті досліджено позитивний вплив цифровізації на національну економіку у секторальному розрізі. Розкрито вплив домінантних тенденцій цифрової трансформації економіки на формування цифрових розривів і дисбалансів у впровадженні цифрових технологій. Систематизовано переваги та ризики використання штучного інтелекту як домінантної тенденції цифровізації. Визначено внутрішні бар'єри впровадження штучного інтелекту підприємствами в Україні. Ідентифіковано загрози економічній безпеці держави в цифровому середовищі, зокрема загрозу робочим місцям для рутинних професій та ескалацію кіберзлочинності.

Обґрунтовано доцільність доповнення показників економічної безпеки держави цифровими індикаторами для розробки дієвих механізмів державної політики цифрового розвитку. Охарактеризовано зміну парадигми економічної безпеки держави та трансформацію пріоритетних напрямів її забезпечення з огляду на необхідність формування технологічного суверенітету та кіберзахисності критичної інфраструктури.

Ключові слова: цифрова трансформація економіки, цифровий розрив, цифровий дисбаланс, штучний інтелект, економічна безпека держави, цифрові ризики, загрози, цифрова нерівність.

УДК 338.2:004.9:338.1

JEL F52, O33, O38

Oleksandra Maslii, PhD in Economics, Associate Professor, Associate Professor of the Department of Finance, Banking and Taxation, National University “Yuri Kondratyuk Poltava Polytechnic”. **Oleksandr Naumenko**, Third-Level Higher Education Applicant (Ph.D. Degree Applicant), National University “Yuri Kondratyuk Poltava Polytechnic”. **The security dimension of dominant trends in the digital transformation of the economy.**

The accelerating pace of digital transformation has fundamentally reshaped the contours of modern economic development, giving rise to both unprecedented opportunities and complex state economic security challenges. This article addresses the multifaceted relationship between dominant digitalization trends and state economic security, with particular emphasis on the structural imbalances and vulnerabilities that emerge in the course of uneven technological adoption. The central problem concerns the dual nature of digital transformation: while enhancing productivity, competitiveness, and public service delivery, it simultaneously generates digital divides and systemic imbalances that undermine national economic resilience. The study examines the positive effects of digitalization across sectoral dimensions of the national economy, identifying areas where digital technologies have generated measurable gains in efficiency and economic output. Special attention is devoted to artificial intelligence as the dominant trend of contemporary digitalization. The article systematizes the advantages and risks associated with AI adoption, offering a structured analysis of its transformative potential alongside the barriers that currently impede its widespread implementation by Ukrainian enterprises. These barriers encompass infrastructural deficiencies, insufficient digital competencies of the workforce, limited access to financing, and the absence of comprehensive regulatory frameworks governing AI deployment in the business environment. The article identifies major threats to state economic security within the digital environment. Among the most significant are the displacement of workers employed in routine occupations due to automation, the escalating sophistication and frequency of cybercrime, and the growing technological dependence on foreign digital platforms and infrastructure. These threats are considered not in isolation but as interconnected elements of a broader systemic risk landscape that demands a coordinated policy response. The article substantiates the necessity of supplementing existing state economic security indicators with digital metrics as a foundation for developing effective digital development policy mechanisms. A central contribution of this research lies in characterizing the paradigm shift within the conceptual framework of state economic security, establishing that its provision must be reconfigured around the imperatives of technological sovereignty and the cyber protection of critical infrastructure. The findings underscore the urgency of embedding digital security considerations into the strategic architecture of national economic policy.

Key words: digital transformation of the economy, digital divide, digital imbalance, artificial intelligence, economic security of the state, digital risks, digital threats, digital inequality.