

Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292. Ефективна економіка. 2025. № 11.

DOI: <http://doi.org/10.32702/2307-2105.2025.11.53>

УДК 338.27:004(477)

С. В. Козловський,

д. е. н., професор,

Донецький національний університет імені Василя Стуса, м. Вінниця

ORCID ID: <https://orcid.org/0000-0003-0707-4996>

І. О. Криворучко,

к. ю. н., Вінницький кооперативний інститут, м. Вінниця

ORCID ID <https://orcid.org/0009-0008-2887-0346>

М. М. Романова,

студентка, Донецький національний університет імені Василя Стуса, м. Вінниця

ORCID ID: <https://orcid.org/0009-0005-8483-345X>

С. О. Горун,

аспірант, Донецький національний університет імені Василя Стуса

м. Вінниця, ORCID: <https://orcid.org/0009-0002-0850-509X>

Д. Ю. Ноздрін,

аспірант, Донецький національний університет імені Василя Стуса

м. Вінниця, ORCID: <https://orcid.org/0009-0004-4764-1320>

ФОРМУВАННЯ МОДЕЛІ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ДЕРЖАВИ НА ОСНОВІ ЦИФРОВИХ ТЕХНОЛОГІЙ

S. Kozlovskiy,
*Doctor of Economic Sciences, Professor,
Vasyl' Stus Donetsk National University, Vinnytsia*

I. Kryvoruchko,
PhD in Law, Vinnytsia Cooperative Institute, Vinnytsia

M. Romanova,
Student, Vasyl' Stus Donetsk National University, Vinnytsia

S. Horun,
Postgraduate student, Vasyl' Stus Donetsk National University, Vinnytsia

D. Nozdrin,
Postgraduate student, Vasyl' Stus Donetsk National University, Vinnytsia

FORMATION OF A MODEL OF ENSURING THE ECONOMIC SECURITY OF THE STATE BASED ON DIGITAL TECHNOLOGIES

У статті досліджується комплексна проблема формування моделі забезпечення економічної безпеки держави на основі цифрових технологій в умовах зростаючих глобальних загроз, кіберконфліктів та цифрової трансформації економіки, де цифровізація набуває особливого значення як критичний інструмент виживання держави під час повномасштабної війни. Проаналізовано чотири моделі цифрової економічної безпеки: естонську модель електронного урядування з найвищою ефективністю через платформу X-Road та universal digital ID, сингапурську модель економіки зі штучним інтелектом з систематичним впровадженням ШІ в бізнес-секторі, регуляторну модель ЄС зі значним фінансуванням та стандартизацією через GDPR і AI Act, та українську модель стійкості в кризі з безпрецедентним зростанням цифровізації в умовах війни. Встановлено, що Україна здійснила стрибок у цифровізації державних послуг за шість років, піднявшись зі 102-го на 5-те місце в рейтингу онлайн-послуг ООН, при цьому платформа Дія забезпечує значну економію бюджетних коштів та сприяє радикальному зниженню тіньової економіки, однак виявлено критичний дисба-

ланс: IT-сектор забезпечує лівову частку експорту послуг, але витрати на кібербезпеку залишаються в кілька разів меншими порівняно з провідними країнами. Детально проаналізовано структуру та динаміку кіберзагроз, що демонструє експоненційне зростання атак на державні органи, критичну інфраструктуру та сектор безпеки. Запропоновано стратегію формування гібридної моделі для України, що синтезує естонську архітектуру електронного урядування, сінгапурський галузевий підхід до впровадження штучного інтелекту в МСП та європейське фінансування через механізм для України з імплементацією регуляторних стандартів ЄС. Унікальною конкурентною перевагою України визначено доведену стійкість – здатність підтримувати функціонування цифрових послуг під масштабними кіберзагрозами та обстрілами інфраструктури, що створює унікальну експертизу у цифровому управлінні під час війни, затребувану глобально в контексті зростаючої нестабільності. Доведено, що економічна безпека України в цифрову епоху потребує формування гібридної моделі, що поєднує міжнародні стандарти з унікальною експертизою функціонування в кризових умовах, адаптивного управління та стратегічного планування в контексті повоєнної відбудови з вбудованою цифровізацією.

The article investigates the complex problem of forming a model for ensuring the state's economic security based on digital technologies in the context of growing global threats, cyber conflicts, and digital transformation of the economy, where digitalization acquires special significance as a critical instrument for state survival during full-scale war. Four models of digital economic security are analyzed: the Estonian e-government model with the highest efficiency through the X-Road platform and universal digital ID, the Singaporean AI economy model with systematic implementation of AI in the business sector, the EU regulatory model with significant financing and standardization through GDPR and AI Act, and the Ukrainian resilience model with unprecedented growth of digitalization under wartime conditions. It was established that Ukraine made the most dramatic leap in digitalization of government services over six years, rising from 102nd to 5th place in the UN Online Services Index, with the Diia

platform providing significant budget savings and contributing to a radical reduction of the shadow economy, however, a critical imbalance was identified: the IT sector provides the lion's share of service exports, but cybersecurity spending remains several times lower compared to leading countries. The structure and dynamics of cyber threats are analyzed in detail, demonstrating exponential growth of attacks on government bodies, critical infrastructure, and the security sector. A strategy for forming a hybrid model for Ukraine is proposed, synthesizing Estonian e-government architecture, Singaporean sectoral approach to AI implementation in SMEs, and European financing through the Ukraine Facility with implementation of EU regulatory standards. Ukraine's unique competitive advantage is identified as proven resilience — the ability to maintain the functioning of digital services under massive cyber threats and infrastructure shelling, creating unique expertise in wartime digital governance that is globally in demand in the context of growing instability. The authors conclude that Ukraine's economic security in the digital age requires the formation of a hybrid model combining international standards with unique expertise in crisis operations, adaptive management, and strategic planning in the context of post-war reconstruction with embedded digitalization.

Ключові слова: економічна безпека держави, модель економічної безпеки, цифрові технології, цифрова трансформація, кібербезпека, електронне урядування, платформа Дія, штучний інтелект, блокчейн, big data, IT-сектор України, міжнародний досвід, тіньова економіка.

Keywords: economic security of the state, economic security model, digital technologies, digital transformation, cybersecurity, e-government, Diia platform, artificial intelligence, blockchain, big data, IT sector of Ukraine, international experience, shadow economy.

Постановка проблеми. Ще десять років тому економічна безпека держави асоціювалась переважно з контролем інфляції, стабільністю валютного курсу та охороною стратегічних об'єктів. Сьогодні ж виявляється, що найбільша загроза

може прийти не від фізичного вторгнення, а від кількох рядків шкідливого коду [1-5]. Кібератаки паралізують банківські системи швидше, ніж будь-які санкції. Віруси-зидники блокують критичні бази даних ефективніше, ніж фізичне знищення серверів. І якщо раніше для дестабілізації економіки потрібна була армія, то тепер достатньо кваліфікованої групи хакерів та правильно організованої інформаційної кампанії.

Цифри вражають, але водночас і лякають своєю абстрактністю. CERT-UA [6] повідомляє про зростання кіберінцидентів на 48% лише за півріччя – але що це насправді означає? Це означає, що кожного дня українські державні системи відбивають сотні атак, про які пересічний громадянин навіть не здогадується. Сінгапур блокує 152 мільйони шахрайських дзвінків на рік – це майже 20 спроб на кожного мешканця щороку. А дефіцит 4 мільйонів спеціалістів з кібербезпеки в ЄС означає, що навіть найбагатші країни світу фізично не встигають готувати фахівців так швидко, як зростають загрози.

Найцікавішим кейсом є Україна. Стрибок зі 102-го на 5-те місце в рейтингу цифровізації за шість років – це не планомірна реформа, це швидше реакція виживання. Війна змусила державу еволюціонувати з неймовірною швидкістю: коли фізична інфраструктура під обстрілами, цифрові сервіси стають не просто зручністю, а необхідністю. Дія з її 20 мільйонами користувачів – це вже не просто додаток, це паралельна державна інфраструктура, яку важче знищити, ніж фізичні будівлі [7-9].

Актуальність дослідження посилюється революційними змінами у сфері штучного інтелекту. Наприклад, у 2024 році Сінгапур зафіксував зростання використання штучного інтелекту серед малих та середніх підприємств у три рази (з 4,2% до 14,5% за один рік) та зростання до 62,5% серед великих компаній [20]. Генеративний штучний інтелект, автономні системи та нові технології створюють як нові можливості для захисту економіки (прогнозна аналітика загроз, автоматизоване реагування на інциденти, удосконалені методи шифрування), так і нові вразливості (шахрайство з використанням технологій глибокої підробки, кі-

бератаки керовані штучним інтелектом, маніпуляції з використанням великих мовних моделей).

Таким чином, формування ефективної моделі забезпечення економічної безпеки держави на основі цифрових технологій є не лише актуальною науковою проблемою, але й критичним практичним завданням для національної безпеки в умовах цифрової трансформації глобальної економіки.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення економічної безпеки в умовах цифровізації перебуває на перетині декількох наукових напрямів і активно досліджується як вітчизняними, так і зарубіжними науковцями. Теоретичні основи економічної безпеки держави розроблено у працях О.М. Ляшенка, В.М. Гейця, М.О. Кизима, Т.С. Клебанової, О.І. Черняка. Цифрову трансформацію та її вплив на фінансову безпеку держави досліджували О. Маслій, А. Максименко. Міжнародний досвід цифровізації ґрунтовно проаналізовано у звітах OECD, UN E-Government Survey, IMDA Singapore, e-Governance Academy. Кібербезпеку та цифрову безпеку держави досліджують CERT-UA, ENISA, ITU Global Cybersecurity Index. Розвиток українського IT-сектору та його вплив на економічну безпеку аналізується у дослідженнях IT Ukraine Association, Civitta, Міністерства цифрової трансформації України. Регуляторні аспекти та фінансування цифрової трансформації в контексті європейської інтеграції розглянуто у документах Європейської Комісії. Попри значний доробок, більшість досліджень фокусуються або на технологічних аспектах цифровізації, або на традиційних підходах до економічної безпеки, не інтегруючи ці напрями в комплексну модель. Бракує системного порівняльного аналізу міжнародних моделей цифрової економічної безпеки та визначення оптимальної стратегії для України з урахуванням воєнного стану та євроінтеграційних процесів.

Метою даного дослідження є формування комплексної моделі забезпечення економічної безпеки держави на основі цифрових технологій шляхом порівняльного аналізу міжнародного досвіду та виявлення універсальних принципів ефективної цифрової трансформації в контексті національної економічної безпеки.

Виклад основного матеріалу дослідження. Економічна безпека держави у ХХІ столітті трансформується під впливом глобальної цифровізації настільки радикально, що традиційні підходи вже не можуть функціонувати ізольовано. До класичних інструментів - монетарної політики, фінансового регулювання, фізичного захисту інфраструктури - додається новий, принципово важливий вимір: кіберстійкість економічних систем та цифровий суверенітет держави. Цифрові технології радикально змінюють як характер загроз (кібератаки на банківську систему, шифрування критичних баз даних, маніпуляції з цифровими активами), так і можливості захисту (системи моніторингу в реальному часі, прогнозна аналітика на основі великих даних, автоматизоване виявлення аномалій).

Сучасні моделі економічної безпеки базуються на трьох взаємопов'язаних концепціях, кожна з яких критична сама по собі, але працює ефективно лише в комплексі.

Цифровий суверенітет означає здатність держави контролювати власний цифровий простір – від захисту даних громадян до незалежності у прийнятті рішень щодо цифрової інфраструктури. Без цього держава перетворюється на заручницю зовнішніх технологічних платформ.

Кіберстійкість економіки – це не просто захист від атак, а здатність системи продовжувати функціонувати навіть під час масованих кібератак. Різниця принципова: не уникнути атаки (це неможливо), а залишитися працездатною попри неї.

Цифрова довіра замикає трикутник. Якщо громадяни та бізнес не довіряють цифровим системам ідентифікації, електронним підписам чи онлайн-транзакціям, жодна цифрова трансформація неможлива - користувачі просто не перейдуть у цифровий простір.

Показово, як змінювалися підходи до захисту протягом останніх тридцяти років. У 1990-2000-х роках захист був реактивним та примітивним: антивірус плюс міжмережевий екран – і цього вважалося достатньо. Сьогодні цей підхід виглядає наївним. Сучасна система безпеки – це багаторівнева інтегрована інфраструктура: штучний інтелект аналізує моделі загроз у реальному часі, блок-

чейн захищає критичні дані від підміни, біометрія замінює паролі, автоматичні системи реагують на інциденти швидше за людину. Революційні зміни 2024 року, зокрема зростання використання штучного інтелекту у три рази серед малого та середнього бізнесу Сінгапуру за один рік, свідчать про масштабну трансформацію підходів. Акцент зміщується від реактивного реагування на інциденти до проактивного прогнозування та превентивної нейтралізації загроз на основі аналізу великих даних [20].

Ключовим елементом сучасних моделей економічної безпеки є комплексна інтеграція цифрових технологій у всі ланки державного управління. Цифровізація державних послуг не лише підвищує ефективність та знижує витрати, але й створює додатковий рівень захисту від корупції завдяки прозорості та відстежуваності всіх операцій. Електронна ідентифікація громадян дозволяє побудувати надійну систему контролю доступу до економічно критичних ресурсів та запобігти шахрайству. Цифрові реєстри на основі блокчейну забезпечують незмінність та достовірність критично важливих даних про власність, ліцензії, дозволи, що є фундаментом економічної стабільності [10-11].

Втім, теорія – це одне, а практична реалізація – зовсім інше. Міжнародний досвід демонструє, що не існує єдиного "правильного" шляху побудови цифрової економічної безпеки. Моделі кардинально різняться: за ступенем централізації управління, набором технологій, правовою базою, рівнем інтеграції з приватним сектором. Показово, що успіху досягають і естонська децентралізована модель, і сінгапурська високоцентралізована, і європейська федеративна. Питання не в копіюванні, а в адаптації універсальних принципів до конкретного національного контексту. Аналіз провідних світових практик дозволяє виокремити як універсальні принципи, так і специфічні рішення для конкретних національних контекстів.

Для порівняльного аналізу обрано Європейський Союз як модель федеративної інтеграції з найсильнішою правовою базою. Не національна модель, а наднаціональна регуляторна рамка для 27 країн-членів. Структура моделі ЄС представлена на рисунку 1.

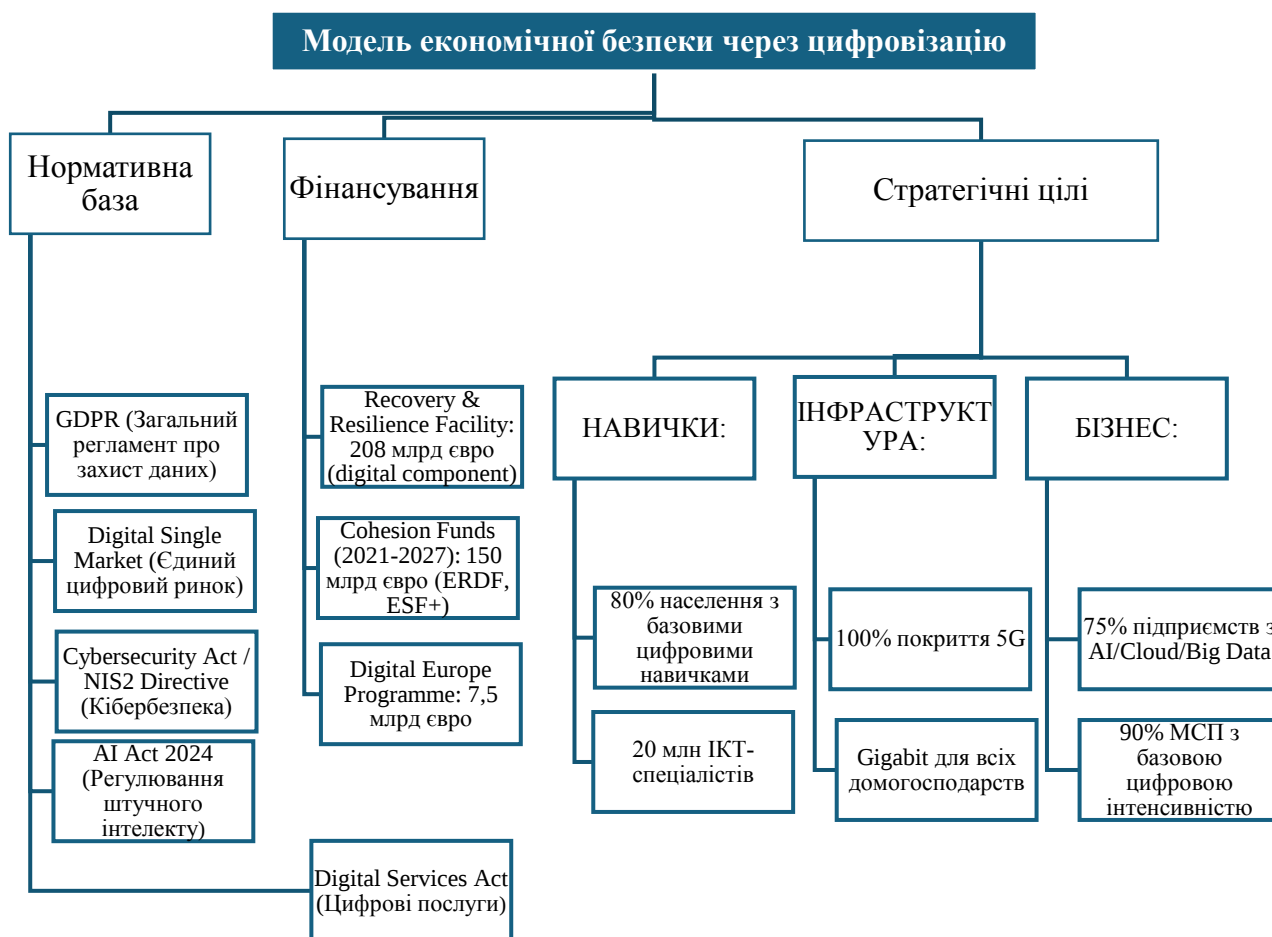


Рис. 1. Модель економічної безпеки через цифровізацію ЄС

Нормативна база ЄС – це спроба створити економічну безпеку через стандартизацію для 450 мільйонів громадян та 25+ мільйонів підприємств. GDPR став де-факто глобальним стандартом захисту даних - будь-яка компанія, що працює з європейцями, змушена його дотримуватись. Це і є технологічний суверенітет: не власні технології, а власні правила гри. Закон про штучний інтелект 2024 року - перша у світі спроба комплексно регулювати ШІ. Системи класифікуються за рівнем ризику, високоризиковані застосування отримують жорсткі вимоги. Критики вказують, що закон може загальмувати інновації, прихильники наголошують на необхідності превентивного регулювання. Час покаже, хто має рацію. Закон про кібербезпеку та Директива NIS2 створюють єдині стандарти кібербезпеки для критичної інфраструктури, обов'язкові для всіх держав-членів. Єдиний цифровий ринок усуває цифрові бар'єри між країнами, створюючи єдиний ринок для електронної комерції, цифрових послуг та даних. Для України ім-

плементация цієї нормативної бази є обов'язковою умовою вступу до ЄС, що вже частково реалізується через законодавчу гармонізацію у сферах захисту даних, кібербезпеки та електронних підписів [13, 14].

Фінансування ЄС на цифровізацію вражає масштабом: понад 365 млрд євро на 2021-2027 роки. Це комбінація Recovery and Resilience Facility (208 млрд євро), Фондів згуртування (150 млрд євро) та Програми «Цифрова Європа» (7,5 млрд євро). Для порівняння – це більше, ніж весь ВВП України за рік.

Центральним елементом української моделі економічної безпеки є екосистема Дія – інтегрована платформа цифрових послуг, що включає мобільний додаток, веб-портал та інфраструктуру для цифрової ідентифікації [13].

Таблиця 1. Дія: вплив на економічну безпеку [13]

Показник	2020	2022	2024	2025 (план)
Користувачі Дії, млн	запуск	~15	~20	25-30
% населення	0%	~35%	42%	55%+
Кількість послуг	<10	72	80+	170+
Бізнесів зареєстровано через Дію (тис.)	~50	~400	~800	1,000+
Економія для громадян, млрд/рік	~46	~46	~46	~46
Номінальний ВВП, трлн грн	4,19	5,19	7,66	~8,5
Тіньова економіка, % ВВП	30%	32%	19,3%	15%
Частка ІТ у ВВП	2,02%	4,9%	4.4%	5%+

Таблиця 1 розкриває трансформацію Дії з технологічного експерименту у стратегічну інфраструктуру. Кількість користувачів зросла з нуля у 2020 році до 20 мільйонів у 2024-му.

Але найцікавіший ефект – вплив на тіньову економіку. Через Дію зареєстровано понад 800 000 бізнесів станом на 2024 рік проти приблизно 50 000 у 2020 році – зростання у 16 разів. Результат: тіньова економіка скоротилася з 30% ВВП (2020-2022) до 19,3% у 2024 році за даними ЕУ. Падіння на 10,7 процентних пунктів під час війни - це аномалія. Зазвичай війни збільшують тіньовий сектор, а не зменшують [13].

Інвестиції в кібербезпеку зросли зі 122 мільйонів доларів у 2023 році до 138 мільйонів у 2024-му, прогноз на 2025 рік – понад 200 мільйонів. Ці витрати

вимушені – вони не створюють нової вартості, а лише захищають існуючу. Фактично це податок на війну, який відволікає ресурси від відновлення економіки. Пріоритетними цілями кібератак є органи державної влади, сектор безпеки і оборони, критична інфраструктура (енергетика, транспорт, зв'язок) та органи місцевого самоврядування. 19 грудня 2024 року росія провела одну з наймасштабніших кібератак на Україну. Частково були порушені сервіси Дії: бронювання працівників, реєстрація ТОВ, онлайн-шлюб, реєстрація прав власності, перереєстрація автомобілів. Систему відновили протягом кількох годин, але сам факт успішної атаки на Дію – найбільш захищену цифрову систему України – демонструє межі можливостей захисту. Абсолютної кібербезпеки не існує.

ІТ-сектор України перетворився на стратегічний елемент економічної безпеки в умовах війни, забезпечуючи критичні валютні надходження (42,6% експорту послуг) та компенсуючи втрати в традиційних галузях, постраждалих від руйнування інфраструктури.

Таблиця 2. ІТ-сектор: макроекономічний вплив та виклики

Показник	2023	2024	2025 (прогноз)
Частка ІТ у ВВП	4,9%	4,4%	5%+
Загальний економічний ефект, \$ млрд	12,7	12,1	13,9+
Експорт ІТ-послуг, \$ млрд	6,7	6,45	7+
Частка ІТ у експорті послуг	42%	37,4%	42,1%
Податкові надходження від ІТ, млрд грн	35,9	37	40+
ІТ-фахівців в Україні (тис)	285 450	282 939	298 461

Таблиця 2 показує парадоксальну динаміку. Частка ІТ у ВВП: 4,9% у 2023 році, 4,4% у 2024-му, прогноз понад 5% у 2025-му. Падіння у 2024 році виглядає дивно на тлі загального зростання сектору. Пояснення - у знаменнику: номінальний ВВП зріс швидше через інфляцію, тому частка ІТ зменшилася. Це статистична ілюзія, а не реальне скорочення сектору [19]. Загальний економічний ефект ІТ-індустрії: 12,7 мільярдів доларів у 2023 році, падіння до 12,1 мільярдів у 2024-му через геополітичну нестабільність та мобілізацію кадрів. Прогноз на 2025 рік - понад 13,9 мільярдів завдяки зростанню експорту та розширенню Дія.Сіті.

Український досвід дійсно унікальний – здатність підтримувати цифрові послуги під понад 6 000 кібератаками щорічно та систематичними обстрілами енергетичної інфраструктури. Це створює експертизу у цифровому управлінні в екстремальних умовах [16-18].

Чи може ця експертиза стати комерційною перевагою? Теоретично - так. Експорт українських моделей, консалтинг для країн у кризових ситуаціях, позиціонування як випробувального майданчика - все це звучить логічно. Але практично - виникають питання:

1. Скільки країн готові платити за досвід цифровізації під час війни?
2. Чи масштабуються українські рішення для інших контекстів?
3. Чи не втратимо ми цю експертизу з завершенням війни, коли фахівці переорієнтуються на відбудову?

Висновок. Український досвід цифровізації під час війни дійсно унікальний. Здатність функціонувати під тисячами кібератак та обстрілами інфраструктури створює експертизу, затребувану в контексті зростаючої глобальної нестабільності. Але трансформація цієї експертизи у комерційну перевагу потребує окремої стратегії - від експорту моделей до консалтингу та позиціонування України як випробувального майданчика стійких рішень. Головний виклик – не втратити досягнуте. Цифровізація в умовах війни відбувалася під тиском необхідності. Після війни цей тиск зникне, а разом з ним може зникнути і темп трансформації. Питання не в тому, чи зможе Україна побудувати гібридну модель, а в тому, чи вистачить політичної волі та ресурсів підтримувати її після завершення гострої фази конфлікту.

Література

1. UN E-Government Survey 2024: Forging Digital Governments for Sustainable Future. United Nations Department of Economic and Social Affairs, 2024. URL: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024>

2. Global Cybersecurity Index 2024. International Telecommunication Union (ITU), 2024. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
3. Singapore Digital Economy Report 2024. Infocomm Media Development Authority (IMDA), 2024. URL: <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/ar-sgde-2024>
4. State of the Digital Decade 2025. European Commission, 2025. URL: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en
5. Recovery and Resilience Facility. European Commission, 2024. URL: https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en
6. CERT-UA. Звіт про кіберінциденти в Україні за 2024 рік. Державна служба спеціального зв'язку та захисту інформації України, 2024. URL: <https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006>
7. Shadow economy exposed: Estimates for the world and policy paths. Ernst & Young Global Limited, March 2025. URL: <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/tax/documents/ey-gl-shadow-economy-report-02-2025.pdf>
8. IT Ukraine Association. Ukraine's IT Exports Declined by Over 4% in 2024. What's Next? IT Ukraine Association, 2025. URL: <https://itukraine.org.ua/en/ukraine-s-it-exports-declined-by-over-4-in-2024-what-next/>
9. e-Governance Academy. Digital Transformation Index 2024. e-Governance Academy Estonia, 2024. URL: <https://ega.ee/>
10. Digital Tiger: The Market Power of Ukrainian IT — 2024. Ministry of Digital Transformation of Ukraine, 2024. URL: <https://digitalstate.gov.ua/news/it-outsourcing/ukraines-it-powerhouse-2024-from-resilience-to-global-reach>
11. Scaling Up: Accelerating Ukraine's Tech Sector. Civitta, u.ventures, Ukraine-Moldova American Enterprise Fund, September 2024. URL:

<https://civitta.com/wp-content/uploads/2024/09/Scaling-Up-accelerating-Ukraines-Tech-Sector.pdf>

12. Національний банк України. Статистика експорту послуг за 2023-2024 роки. НБУ, 2025. URL: <https://bank.gov.ua/>
13. Міністерство цифрової трансформації України. Звіт про розвиток екосистеми Дія 2020-2024. Мінцифри України, 2024. URL: <https://diia.gov.ua/>
14. OECD Digital Economy Outlook 2024. Organisation for Economic Co-operation and Development, 2024. URL: <https://www.oecd.org/digital/oecd-digital-economy-outlook.htm>
15. Eurostat. Digital Economy and Society Statistics 2024. European Statistical Office, 2024. URL: <https://ec.europa.eu/eurostat/>
16. Ляшенко О. М. Концептуалізація управління економічною безпекою підприємства: монографія. Луганськ: СНУ ім. В. Даля, 2011. 400 с. URL: https://niss.gov.ua/sites/default/files/2015-10/lyashenko_1_druk-43fc7.pdf
17. Гейць В. М., Кизим М. О., Клебанова Т. С., Черняк О. І. Моделювання економічної безпеки: держава, регіон, підприємство: монографія / За ред. В. М. Гейця. Харків: ВД «ІНЖЕК», 2006. 240 с.
18. Маслій О., Максименко А. Цифрова трансформація та економічна деіндустріалізація: вплив на фінансову безпеку держави. Фінансово-кредитна діяльність: проблеми теорії і практики. 2025. № 1 (60). С. 401-414. URL: <https://fkд.net.ua/index.php/fkd/article/view/4599>
19. ENISA Threat Landscape Report 2024. European Union Agency for Cybersecurity, 2024. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
20. Singapore Ministry of Digital Development and Information. National AI Strategy 2.0. MDDI Singapore, 2023. URL: <https://www.smartnation.gov.sg/initiatives/artificial-intelligence/>

References

1. United Nations Department of Economic and Social Affairs (2024), “UN E-Government Survey 2024: Forging Digital Governments for Sustainable Future”, available at: <https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2024> (Accessed 10 Oct 2025).
2. International Telecommunication Union (ITU) (2024), “Global Cybersecurity Index 2024”, available at: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> (Accessed 10 Oct 2025).
3. Infocomm Media Development Authority (IMDA) (2024), “Singapore Digital Economy Report 2024”, available at: <https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/factsheets/2024/ar-sgde-2024> (Accessed 10 Oct 2025).
4. European Commission (2025), “State of the Digital Decade 2025”, available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en (Accessed 10 Oct 2025).
5. European Commission (2024), “Recovery and Resilience Facility”, available at: https://commission.europa.eu/business-economy-euro/economic-recovery/recovery-and-resilience-facility_en (Accessed 10 Oct 2025).
6. State Service of Special Communications and Information Protection of Ukraine (2024), “Report on cyber incidents in Ukraine for 2024”, available at: <https://scpc.gov.ua/api/files/72e13298-4d02-40bf-b436-46d927c88006> (Accessed 10 Oct 2025).
7. Ernst & Young Global Limited (2025), “Shadow economy exposed: Estimates for the world and policy paths”, available at: <https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/tax/documents/ey-gl-shadow-economy-report-02-2025.pdf> (Accessed 10 Oct 2025).

8. IT Ukraine Association (2025), “Ukraines IT Exports Declined by Over 4% in 2024. Whats Next?”, available at: <https://itukraine.org.ua/en/ukraine-s-it-exports-declined-by-over-4-in-2024-what-next/> (Accessed 10 Oct 2025).
9. e-Governance Academy Estonia (2024), “Digital Transformation Index 2024”, available at: <https://ega.ee/> (Accessed 10 Oct 2025).
10. Ministry of Digital Transformation of Ukraine (2024), “Digital Tiger: The Market Power of Ukrainian IT — 2024”, available at: <https://digitalstate.gov.ua/news/it-outsourcing/ukraines-it-powerhouse-2024-from-resilience-to-global-reach> (Accessed 10 Oct 2025).
11. Ukraine-Moldova American Enterprise Fund (2024), “Scaling Up: Accelerating Ukraines Tech Sector. Civitta, u.ventures”, available at: <https://civitta.com/wp-content/uploads/2024/09/Scaling-Up-accelerating-Ukraines-Tech-Sector.pdf> (Accessed 10 Oct 2025).
12. National Bank of Ukraine (2025), “Services Export Statistics for 2023-2024”, available at: <https://bank.gov.ua/> (Accessed 10 Oct 2025).
13. Ministry of Digital Transformation of Ukraine (2024), “Report on the Development of the Ecosystem Diia 2020-2024”, available at: <https://diia.gov.ua/> (Accessed 10 Oct 2025).
14. Organisation for Economic Co-operation and Development (2024), “OECD Digital Economy Outlook 2024”, available at: <https://www.oecd.org/digital/oecd-digital-economy-outlook.htm> (Accessed 10 Oct 2025).
15. European Statistical Office (2024), “Digital Economy and Society Statistics 2024”, available at: <https://ec.europa.eu/eurostat/> (Accessed 10 Oct 2025).
16. Liashenko, O.M. (2011), Kontseptualizatsiia upravlinnia ekonomichnoiu bezpekoiu pidpryiemstva [Conceptualization of the management of economic security of the enterprise], SNU im. V. Dalia, Luhansk, Ukraine, available at: https://niss.gov.ua/sites/default/files/2015-10/lyashenko_1_druk-43fc7.pdf (Accessed 10 Oct 2025).

17. Heits, V.M. Kyzym, M.O. Klebanova, T.S. and Cherniak, O.I. (2006), Modeliuvannia ekonomichnoi bezpeky: derzhava, rehion, pidpriemstvo [Modeling of economic security: state, region, enterprise], VD «INZhEK», Kharkiv, Ukraine.
18. Masliim, O. and Maksymenkom, A. (2025), “Digital transformation and economic de-industrialization: impact on the financial security of the state”, Finansovo-kredytna diialnist: problemy teorii i praktyky, vol. 1 (60), pp. 401-414, available at: <https://fkd.net.ua/index.php/fkd/article/view/4599> (Accessed 10 Oct 2025).
19. European Union Agency for Cybersecurity (2024), “Threat Landscape Report 2024”, available at: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024> (Accessed 10 Oct 2025).
20. Singapore Ministry of Digital Development and Information (2023), “National AI Strategy 2.0”, available at: <https://www.smartnation.gov.sg/initiatives/artificial-intelligence/> (Accessed 10 Oct 2025).

Стаття надійшла до редакції 21.10.2025 р.