

ДЕСТРУКТИВНЕ ЦИФРОВЕ ПІДПРИЄМНИЦТВО У ФОРМУВАННІ СИСТЕМНОЇ ВРАЗЛИВОСТІ ЕКОНОМІКИ УКРАЇНИ: ВИКЛИКИ ДЛЯ РЕЗИЛЬЄНТНОСТІ ТА БЕЗПЕКИ РОЗВИТКУ

Ю. В. Кіндзерський, д. е. н., старший науковий співробітник, провідний науковий співробітник відділу інноваційної політики, економіки та організації високих технологій ДУ «Інститут економіки та прогнозування НАН України», Kindzerskyi@nas.gov.ua, orcid.org/0000-0002-4432-6526

Методологія дослідження. Застосовано інституційний, системний і порівняльний підходи, причинно-наслідковий аналіз та метод аналітичної типологізації. Деструктивність цифрової бізнес-моделі оцінено за структурою приватного стимулу, способом екстерналізації суспільної шкоди та здатністю створювати системну незамінність; резильєнтність – за спроможністю економіки, суспільства і держави зберігати критичні функції, адаптуватися та відновлюватися після шоку.

Результати. Уточнено зміст деструктивного цифрового підприємництва та відмежовано його від технологічного ризику, цифрового розриву, кримінальної діяльності й зовнішньої залежності. Систематизовано механізми ринкової влади, інформаційної асиметрії, поведінкової експлуатації, екстерналізації ризику, регуляторного арбітражу і технологічного замикання. Розкрито їх вплив на економічну, технологічну, соціальну та інформаційну резильєнтність. Порівняно підходи ЄС і США та визначено критичні для України цифрові ризики воєнного часу і повоєнної відбудови. Показано, що висока приватна ефективність цифрової моделі не гарантує суспільної стійкості, якщо разом зі зниженням поточних витрат звужуються альтернативи, резерви, компетентності й канали відновлення. Визначено межу між керованою взаємозалежністю та рентною незамінністю постачальника.

Новизна. Запропоновано наскрізну конструкцію переходу від приватного стимулу через бізнес-практику і негативний зовнішній ефект до системної вразливості та зниження резильєнтності економіки. Обґрунтовано, що цифрову автономію України доцільно розуміти не як автаркію, а як керованість критичних залежностей і збереження свободи критичного рішення.

Практична значущість. Сформовано орієнтири для конкурентної, закупівельної, інноваційної, соціальної, інформаційної та безпекової політики. Запропоновано діагностичний тест для регулятора й державного замовника, побудований на оцінюванні незамінності постачальника, переносимості даних, можливості оскарження, розподілу вартості помилки, резервування та безперервності критичної функції.

Ключові слова: деструктивне підприємництво, цифрові бізнес-моделі, резильєнтність, системна вразливість, національна безпека, технологічна залежність, цифрові платформи, штучний інтелект, державне регулювання, повоєнна відбудова.

Постановка проблеми. У сучасній економічній теорії підприємництво переважно пов'язується з пошуком нових можливостей, інноваціями, створенням ринків і підвищенням продуктивності. Проте така інтерпретація є неповною, якщо результат підприємницької діяльності оцінювати не лише за приватною дохідністю, а й за тим, яким

способом ця дохідність формується та які витрати при цьому покладаються на інших учасників суспільства. В. Баумоль [1] показав, що підприємницький талант є ресурсом, напрям використання якого визначається інституційними стимулами: за одних правил він спрямовується на створення нової цінності (продуктивне підприємництво), за

інших – на пошук ренти, перерозподіл (непродуктивне підприємництво) або діяльність, що прямо зменшує суспільний добробут (деструктивне підприємництво).

Для цифрової економіки ця постановка набуває особливої ваги, оскільки цифрова бізнес-модель може одночасно охоплювати мільйони користувачів, впливати на конкуренцію, інформаційне середовище, поведінку споживачів, трудові відносини й навіть на функціонування державних та оборонних систем.

Водночас для аналізу стійкості бізнесу у воєнно-повоєнний період критерію суспільної шкоди недостатньо. Важливо простежити, як конкретна деструктивна практика переходить у системну вразливість і знижує резильєнтність економіки. У цьому зв'язку доцільно розглядати наскрізну причинну конструкцію: приватний стимул формує бізнес-практику; практика породжує негативний зовнішній ефект; якщо він концентрується у критичній функції, виникає системна вразливість; накопичення такої вразливості послаблює здатність підприємства, суспільства або держави протистояти шоку, адаптуватися і відновлюватися. Звідси впливає важливе розрізнення трьох типів цифрових моделей. Продуктивна модель поєднує приватну ефективність, позитивний суспільний ефект і зростання резильєнтності. Потенційно вразлива модель може створювати позитивний поточний ефект, але одночасно зменшувати резерви, альтернативність і здатність до відновлення. Деструктивна модель характеризується тим, що її дохідність безпосередньо спирається на створення або екстерналізацію шкоди. Такий підхід не ототожнює крихкість із деструктивністю, але показує, коли приватна оптимізація стає джерелом системної небезпеки [2].

Аналіз останніх досліджень і публікацій. Інституційна постановка проблеми походить від розмежування В. Баумолем продуктивного, непродуктивного й деструктивного підприємництва [1]. У цифровій площині її розвинув В. Науде, який систематизував суспільні ризики цифрової трансформації та показав можливість їх підприємницького масштабування [3]. Дослідження цифрової залежності користувача, інфор-

маційної екосистеми, психосоціальної вразливості, продуктивності праці та перепідготовки розкривають окремі канали впливу цифрових бізнес-моделей [4–8].

Наукові праці ОЕСР, Стенфордського інституту людиноцентричного штучного інтелекту та Світового банку висвітлюють концентрацію обчислювальної інфраструктури, ринкову владу у ланцюгах створення штучного інтелекту, зовнішню технологічну залежність і вимоги до цифрової безпеки [9–13]. Проте в наявних дослідженнях недостатньо розмежовано деструктивну бізнес-модель, структурну вразливість і власне технологічний ризик, а їх зв'язок з резильєнтністю економіки країни не зведено в єдину причинну конструкцію. Для вразливої і ослабленої через війну економіки України уникнення ризиків деструктивного цифрового підприємництва набуває особливої гостроти у воєнно-повоєнний період.

Формулювання мети статті. Метою статті є уточнення змісту деструктивного цифрового підприємництва, розкриття механізму його перетворення на системну вразливість та обґрунтування орієнтирів державної політики щодо збереження резильєнтності й національної безпеки України під час війни та повоєнної відбудови.

Методологія дослідження. Методологічною основою є інституційний і системний підходи. Причинно-наслідковий аналіз використано для переходу від приватного стимулу до системної вразливості; типологізацію – для класифікації механізмів деструктивності; порівняльний аналіз – для зіставлення регуляторних підходів ЄС і США та визначення релевантних для України інструментів.

Виклад основного матеріалу дослідження. Деструктивне цифрове підприємництво доцільно визначати не за видом технології і не за знаком сукупного суспільного результату, а за структурою економічного стимулу. Бізнес-модель є деструктивною тією мірою, якою її приватна дохідність систематично залежить від створення, посилення або перенесення на інших істотної суспільної шкоди. Це визначення передбачає п'ять взаємопов'язаних ознак: існування приватного економічного стимулу; стійкий зв'язок прибутковості з певною практикою;

наявність істотних негативних зовнішніх ефектів; можливість суб'єкта не нести повної вартості створеної ним шкоди; залежність вигоди саме від механізму, який цю шкоду породжує або посилює. Тому корисна в цілому цифрова платформа може містити деструктивний компонент, якщо окрема частина її доходу залежить, наприклад, від нав'язування незамінності, прихованого використання даних або алгоритмічного підсилення конфліктного вмісту. І навпаки, негативний наслідок технології ще не доводить наявності деструктивного підприємництва, якщо він не пов'язаний із відповідною моделлю отримання приватної вигоди.

Таке розмежування принципове. Технологія сама по собі не є підприємницькою практикою; цифровий розрив є структурним станом економіки; психологічне погіршення добробуту – можливим соціальним наслідком; державний нагляд – формою здійснення публічної влади; кіберзлочинність – переважно кримінальною діяльністю; залежність держави від зовнішньої цифрової інфраструктури – характеристикою її виробничо-технологічної структури. Усі ці явища можуть бути пов'язані з деструктивним підприємництвом, але не є його рівнозначними формами. Предметом дослідження мають залишатися ті приватні або змішані бізнес-моделі, у яких ринкова влада, інформаційна асиметрія, поведінкова експлуатація, перенесення ризику, використання регуляторних прогалин або технологічне замикання перетворюються на джерело доходу. Саме таке звуження поняття дозволяє уникнути ситуації, коли до деструктивного підприємництва відносяться майже всі небажані наслідки цифровізації.

Під резильєнтністю розуміється здатність економічної та суспільної системи зберігати критично важливі функції під час шоку, поглинати його наслідки, адаптуватися до зміни умов і відновлюватися без втрати базових можливостей розвитку. Такий підхід дозволяє відрізнити резильєнтність від безпеки: безпека концентрується передусім на загрозах і захисті від них, тоді як резильєнтність – на спроможності системи продовжувати функціонувати, перебудовуватися і відновлюватися після реалізації загрози. У цифровій економіці ці два виміри

дедалі тісніше переплітаються, оскільки порушення роботи цифрового посередника, хмарної інфраструктури, системи даних або алгоритмічного сервісу здатне одночасно породити економічні, соціальні, інформаційні та безпекові наслідки. Саме тому цифрову безпеку доцільно оцінювати не лише як технічний захист інформаційних систем, а як управління економічними й соціальними ризиками, що забезпечує безперервність критичних функцій і довіру до цифрового середовища.

Для аналізу деструктивного цифрового підприємництва доцільно виділити чотири взаємопов'язані складові резильєнтності. Економічна резильєнтність характеризує здатність підтримувати виробництво, обмін, зайнятість, фінансові потоки та конкурентне середовище під час шоків. Технологічна – здатність зберігати доступ до критичних технологій, даних, обчислювальних ресурсів, програмного забезпечення та кваліфікацій, замінювати втрачені елементи і відновлювати технологічні функції. Соціальна – здатність суспільства зберігати довіру, згуртованість, людський капітал, справедливий доступ до базових послуг та можливість адаптації різних соціальних груп. Інформаційна – здатність інформаційного середовища забезпечувати доступ до достовірних відомостей, зберігати автономність суджень громадян і стійкість суспільної комунікації до маніпуляцій. Зовнішня економічна, технологічна та політична залежність не становить окремої п'ятої складової, а є наскрізним параметром усіх чотирьох: вона визначає, якою мірою підтримання критичних функцій залежить від рішень, ресурсів і правил, що формуються поза межами країни.

Такий підхід уточнює критерій деструктивності. Висока приватна ефективність не є достатньою підставою вважати бізнес-модель продуктивною з позицій суспільства. Якщо зростання її ефективності одночасно зменшує різноманітність постачальників, ліквідує резервні можливості, концентрує критичні дані й компетенції в одному вузлі, підвищує витрати переходу або підриває довіру та людські навички, то система може ставати дешевшою і продуктивнішою у звичайному режимі, але крихкішою під час кризи. Водночас сама крих-

кість ще не робить бізнес-модель деструктивною. Деструктивна складова виникає тоді, коли приватна дохідність систематично пов'язана саме з нарощуванням такої крихкості або з перенесенням вартості її наслідків на споживачів, конкурентів, державу чи майбутні покоління.

Звідси випливає, що деструктивне цифрове підприємництво знижує резильєнтність не одним універсальним способом, а через кілька каналів. Воно може концентрувати критичні функції та звужувати резерви; перетворювати інформаційну асиметрію на джерело ренти; робити залежність користувача економічно вигідною для постачальника; екстерналізувати витрати помилок і кібервразливостей; послаблювати здатність людей до автономного рішення через поведінкову експлуатацію; підривати довіру та соціальну згуртованість; а також трансформувати нормальну міжнародну взаємозалежність у асиметричну залежність, за якої зміна зовнішніх комерційних або політичних умов здатна порушити критично важливі функції. У мирній економіці частина цих наслідків може тривалий час залишатися прихованою, тоді як війна різко підвищує ціну одиничної точки відмови, інформаційної маніпуляції, втрати доступу до сервісу чи технологічної незамінності.

Цифрова економіка створює особливо сприятливі умови для масштабування деструктивних стимулів. По-перше, мережеві ефекти та накопичення даних можуть швидко перетворювати перевагу великого учасника на самопосилювану ринкову владу. По-

друге, алгоритмічне посередництво робить механізм впливу на користувача малопомітним: людина або підприємство бачить результат рекомендації, ранжування, оцінювання чи ціноутворення, але часто не може перевірити логіку його формування. По-третє, цифрові екосистеми дозволяють пов'язувати дані, програмні засоби, канали збуту і додаткові послуги так, що витрати переходу до іншого постачальника стають непропорційно високими. По-четверте, транснаціональний масштаб дозволяє використовувати відмінності між юрисдикціями, тоді як регуляторні повноваження залишаються переважно національними. По-п'яте, цифровий продукт має надзвичайно низьку граничну вартість масштабування, тому як корисний, так і шкідливий ефект може поширюватися значно швидше, ніж у традиційній промисловості. Сучасні дослідження конкуренції у сфері штучного інтелекту підтверджують, що концентрація може формуватися одразу на кількох рівнях – обчислювальної інфраструктури, даних, базових моделей і доступу до кінцевого користувача [9; 10].

На рівні конкретних механізмів деструктивності цифрових бізнес-моделей доцільно систематизувати не за окремими технологіями, а за способом перетворення суспільної вразливості на приватну вигоду (табл. 1). Така типологія дозволяє звести різноманітні явища до шести економічно однорідніших механізмів і водночас чітко визначити, за якою ознакою виникають підстави для регуляторного втручання.

Таблиця 1

Механізми деструктивності цифрових бізнес-моделей

Механізм деструктивності	Типова бізнес-практика	Джерело приватної вигоди	Суспільна шкода	Критерій регуляторного втручання
Ринкова влада	Надання переваг власним послугам, контроль доступу до ринку, нав'язування пов'язаних сервісів	Рента від інфраструктурної позиції	Придушення конкуренції, зменшення інноваційної різноманітності	Незамінність посередника, високі бар'єри входу або переходу
Інформаційна асиметрія	Непрозоре ранжування, профілювання, автоматизоване оцінювання	Монетизація даних і перевага від неперевірюваності	Дискримінація, помилки, обмеження можливості захистити право	Неможливість перевірки, відтворення або оскарження рішення

Механізм деструктивності	Типова бізнес-практика	Джерело приватної вигоди	Суспільна шкода	Критерій регуляторного втручання
Поведінкова експлуатація	Маніпулятивний дизайн, максимізація утримання уваги, використання вразливостей	Монетизація часу, реклами та поведінкових даних	Втрата добробуту, поляризація, залежність, погіршення інформаційного середовища	Прибуток систематично зростає разом з експлуатацією вразливості
Екстерналізація ризику	Перенесення наслідків помилки, вразливості або небезпечного застосування на користувача чи державу	Скорочення витрат на безпеку, перевірку і компенсацію шкоди	Соціальні, фінансові, кібернетичні та безпекові втрати	Основну вартість шкоди сплачує третя сторона
Регуляторний арбітраж	Використання прогалів між правовими режимами або заперечення статусу, що тягне зобов'язання	Економія на податках, праці, безпеці, захисті споживача	Нерівна конкуренція, послаблення загальних правил	Систематична вигода від уникнення зобов'язань
Технологічне замикання	Несумісні формати, непереносимість даних, залежність від одного постачальника або комплексу послуг	Рента від залежності й високих витрат виходу	Втрата автономії, системна вразливість, зростання майбутніх витрат	Непропорційна вартість зміни постачальника або відсутність реальної альтернативи

Джерело: складено за [1; 3; 9; 10]

Така систематизація дозволяє негативні прояви цифровізації, які В. Науде називає цифровими дистопіями (табл. 2), розглядати як групи суспільних ризиків, частина яких безпосередньо породжується деструктивними бізнес-моделями, а частина – посилюється ними [3]. Це пов'язує підходи В. Баумоля і В. Науде: перший пояснює, як інститути спрямовують підприємницькі стимули, другий показує, до яких негативних результатів може приводити цифрова трансформація, коли ці стимули налаштовані на приватне привласнення вигід без належного врахування суспільних витрат [1; 3].

Співвідношення між цифровими дистопіями, підприємницькими механізмами та складовими резильєнтності доцільно поєднати в одній матриці (див. табл. 2). Вона показує, що одна й та сама дистопія може впливати відразу на кілька складових стійкості, а одна й та сама деструктивна бізнес-практика – породжувати різні види системної вразливості. Тому розподіл у таблиці не є жорсткою взаємовиключною класифікацією, він лише виокремлює домінуючий канал впливу [3].

Таблиця 2

Цифрові дистопії у координатах резильєнтності та національної безпеки

Дистопія / ризик	Підприємницький механізм	Основна складова резильєнтності	Канал зниження резильєнтності	Зовнішня залежність / безпековий вимір
Цифровий платформний капіталізм	Ринкова влада, технологічне замикання, самоперевага власних сервісів	Економічна; технологічна	Звуження конкуренції та резервних каналів збуту; залежність підприємств від правил одного посередника	Зовнішня економічна і технологічна залежність за домінування іноземних платформ
Технологічна винятковість	Регуляторний арбітраж, уникнення загальних зобов'язань	Економічна; соціальна	Перенесення витрат праці, безпеки та захисту споживача на суспільство; нерівні умови конкуренції	Послаблення спроможності держави встановлювати однакові правила для транснаціональних суб'єктів

ЕКОНОМІКА ТА МІЖНАРОДНІ ЕКОНОМІЧНІ ВІДНОСИНИ (ЗА СПЕЦІАЛІЗАЦІЄЮ)

Дистопія / ризик	Підприємницький механізм	Основна складова резильєнтності	Канал зниження резильєнтності	Зовнішня залежність / безпековий вимір
Держава цифрового нагляду – у підприємницькому вимірі комерціалізація масового спостереження	Надмірне накопичення і монетизація персональних та поведінкових даних	Соціальна; інформаційна	Ерозія приватності й довіри, розширення можливостей профілювання і маніпуляції	Політична вразливість, якщо критичні масиви даних і засоби аналізу контролюються зовнішніми суб'єктами
Цифрова пастка бідності	Інформаційна асиметрія, непрозоре автоматизоване оцінювання	Соціальна; економічна	Закріплення нерівності, помилкове виключення з кредиту, страхування чи допомоги, зниження здатності домогосподарств адаптуватися до шоку	Залежність від зовнішніх моделей оцінювання може посилювати непридатність рішень до українського контексту
Цифрові розриви	Монополізація доступу, завищені витрати переходу, недостатня конкуренція у критичних цифрових послугах	Соціальна; технологічна; економічна	Нерівний доступ до цифрових можливостей, ослаблення людського капіталу та продуктивності регіонів і груп	Посилення зовнішньої технологічної залежності через відсутність власних компетенцій і альтернатив
Втрата смисловування	Монетизація уваги, алгоритмічне підсилення емоційного та поляризуючого вмісту	Інформаційна; соціальна	Зниження якості інформаційного середовища, поляризація, втрата довіри та здатності до колективного рішення	Підвищення вразливості до зовнішнього інформаційного впливу
Цифрова залежність користувача	Поведінкова експлуатація, маніпулятивна архітектура взаємодії	Соціальна; інформаційна	Втрата часу, концентрації та автономності поведінки; послаблення критичного мислення	Залежність від правил і алгоритмів платформ, що не підконтрольні національній юрисдикції
Цифрова депресія та інші психосоціальні наслідки	Прибутковість, пов'язана з максимізацією залучення без урахування вразливості окремих груп	Соціальна	Погіршення психосоціального добробуту, зниження навчальної та трудової спроможності, послаблення згуртованості	Непряма: зовнішні платформи можуть масштабувати наслідки без достатньої локальної підзвітності
Кіберзлочинність – граничний випадок	Комерціалізація викрадених даних, шкідливих програм, шахрайських сервісів	Технологічна; економічна; інформаційна	Порушення безперервності критичних функцій, фінансові втрати, компрометація даних і довіри	Може поєднуватися з зовнішнім кримінальним або ворожим впливом, але виходить за межі легального підприємництва
Небезпечне використання штучного інтелекту	Прискорення профілювання, маніпуляції, автоматизації рішень, кібератак і технологічного замикання	Усі складові	Масштабування помилок і зовнішніх ефектів, концентрація обчислювальної та інформаційної влади	Залежність від моделей, обчислень, даних, програмного забезпечення та правил доступу зовнішніх поставальників

Джерело: складено автором за [3–13]

Перший блок ризиків пов'язаний із платформним капіталізмом і технологічною винятковістю. Платформна влада є найбільш безпосереднім випадком деструктивної цифрової бізнес-моделі тоді, коли посередник одночасно встановлює правила ринку,

контролює дані про його учасників і конкурує з ними. Небезпека полягає не в самому великому розмірі компанії, а у використанні інфраструктурної позиції для надання переваг власним послугам, ускладнення переходу до конкурента, нав'язування невігідних

умов або придбання потенційних конкурентів до того, як вони перетворюються на реальну альтернативу. Технологічна винятковість є іншим боком того самого механізму: новизна продукту використовується як аргумент для перенесення на працівників, споживачів чи державу витрат, які традиційний бізнес мав би нести сам [3; 9; 10]. В обох випадках деструктивність визначається не інноваційністю, а тим, що прибуткова перевага формується завдяки послабленню конкуренції чи уникненню зобов'язань.

Другий блок стосується того, що В. Науде називає державою цифрового нагляду та цифровою пасткою бідності. У першому випадку підприємницьким механізмом є не державний нагляд як такий, а комерціалізація надмірного накопичення, об'єднання та монетизації персональних і поведінкових даних. Постачальник має стимул збирати більше даних, ніж потрібно для основної послуги, оскільки вони розширюють можливості профілювання, реклами, оцінювання ризиків або продажу аналітичних продуктів. Держава може стати користувачем цієї інфраструктури, однак це вже наступний рівень проблеми. У цифровій пастці бідності деструктивність виникає тоді, коли автоматизоване кредитне, страхове, кадрове або соціальне оцінювання дає постачальнику економію на витратах, тоді як вартість помилки чи упередження несе людина, яка часто не має реальної можливості перевірити дані й оскаржити рішення [3; 13]. Отже, спільним механізмом є інформаційна асиметрія та екстерналізація ризику, а не сама автоматизація.

Третій блок охоплює цифрові розриви та зовнішню технологічну залежність. Цифровий розрив сам по собі не є підприємницькою практикою: він може виникати через різницю у доходах, освіті, інфраструктурі, міжнародній спеціалізації чи державній політиці. Деструктивна підприємницька складова з'являється тоді, коли сильніший учасник перетворює вже наявну асиметрію на джерело ренти: обмежує переносимість даних, створює несумісні формати, пов'язує критичну послугу з додатковими продуктами, встановлює непропорційно високі витрати виходу або використовує одностороннє право змінювати умови доступу [3; 12;

13]. Отже, залежність не дорівнює деструктивному підприємництву. Вона стає його середовищем лише тоді, коли постачальник використовує незамінність як економічний актив і отримує дохід від звуження свободи клієнта.

Четвертий блок – втрата смислоутворення та цифрова залежність користувача – найбільш чітко демонструє поведінкову природу деструктивності. Рекламна модель створює стимул збільшувати тривалість і частоту взаємодії користувача із сервісом. Якщо емоційний, конфліктний або неправдивий вміст утримує увагу краще за нейтральний і достовірний, алгоритмічна оптимізація може систематично посилювати поляризацію, не ставлячи такої мети прямо. Сучасні дослідження інформаційної екосистеми показують, що цифрові платформи та штучний інтелект змінюють відносну вартість створення, поширення і перевірки інформації, а отже – структуру стимулів для виробників вмісту. Додатково експериментальні дослідження користування соціальними мережами виявляють ознаки проблем самоконтролю та звички: обмеження користування може давати стійкий ефект, що свідчить про відмінність між формально добровільним вибором і поведінкою, яку цілеспрямовано формує дизайн цифрового продукту [4; 5]. Деструктивність тут виникає там, де прибуток безпосередньо зростає разом із використанням вразливості уваги.

П'ятий блок – цифрова депресія та інші психосоціальні наслідки – слід трактувати ще обережніше. Поки що немає достатньо підстав проголошувати будь-яке користування соціальними мережами шкідливим з точки зору формування негативного психічного стану. Водночас є підстави говорити про можливу деструктивну бізнес-практику, коли платформа свідомо використовує механізми соціального порівняння, невизначеної винагороди, нав'язливих повідомлень чи персоналізованого утримання для збільшення часу користування, хоча має достатні дані про непропорційний ризик для вразливих груп. Як підтверджують дослідження, тимчасове припинення користування соціальними мережами може підвищувати суб'єктивний добробут людини, оскільки мережі мають певні механізми впливу на

погіршення її психічного здоров'я [6]. Відповідно об'єктом регулювання має бути не «поганий психологічний результат» як такий, а економічна модель, яка систематично робить експлуатацію вразливості прибутковою.

Шостий блок – кіберзлочинність – є граничним випадком. Він показує, наскільки цифрові технології знижують вартість масштабування шахрайства, вимагання, торгівлі викраденими даними і шкідливими програмами, але основна частина такої діяльності вже лежить поза межами легальної економіки. Тому кіберзлочинність не варто ставити в центр деструктивного підприємництва; значно важливіше виявляти легальний бізнес, який отримує приватну вигоду завдяки перенесенню суспільних витрат. Разом із тим межа між легальним і нелегальним цифровим ринком може бути проникною: рекламні мережі, хмарні послуги, платіжні інструменти та засоби автоматизації можуть ненавмисно або через слабкі стимули до перевірки підтримувати злочинну інфраструктуру [2; 3]. У такому разі питання полягає вже не в самому злочині, а в тому, чи має легальний посередник економічну мотивацію належно управляти системним ризиком, який виникає на його інфраструктурі.

Нарешті, небезпечний штучний інтелект у класифікації В. Науде доцільно розглядати не як окрему бізнес-модель, а як технологічний прискорювач майже всіх названих механізмів. Він може підвищувати точність профілювання, автоматизувати створення переконливого вмісту, здешевлювати шахрайство, посилювати асиметрію інформації, змінювати ринок праці та збільшувати залежність від обмеженої кількості постачальників. Водночас емпіричні дані підтверджують і значний продуктивний потенціал: у дослідженні масового застосування генеративного штучного інтелекту в обслуговуванні клієнтів продуктивність у середньому зросла, причому найбільший ефект отримали менш досвідчені працівники [7; 8]. Саме тому технологію не можна оцінювати як апіорі деструктивну. Деструктивність виникає там, де комерційне застосування робить вигідним непрозоре перенесення ризику, дискримінаційне рішення,

маніпуляцію, зниження безпеки або технологічне замикання.

Узагальнення дистопій В. Науде через механізми деструктивності дозволяє перейти від опису окремих негативних явищ до аналізу того, як вони змінюють здатність країни протистояти шокам. У цьому ракурсі центральною стає не сама наявність цифрового ризику, а його здатність накопичувати системну вразливість. Одна бізнес-модель може одночасно послаблювати кілька складових резильєнтності, а межі між ними є проникними: економічна концентрація створює технологічну залежність; технологічна залежність може породжувати політичну вразливість; інформаційна маніпуляція руйнує соціальну довіру; соціальна нерівність звужує кадрову та економічну базу відновлення. Саме цей взаємний перехід ризиків пояснює, чому деструктивне цифрове підприємництво в умовах війни має оцінюватися не лише як проблема ринку чи захисту споживача, а як чинник національної резильєнтності.

Деструктивні практики у координа- тах резильєнтності

Найбезпосередніше деструктивні цифрові бізнес-моделі впливають на економічну резильєнтність через концентрацію ринкової влади та перерозподіл доходів на користь інфраструктурного посередника. Платформа (на кшталт, Amazon чи Temu), яка контролює доступ до аудиторії, дані про попит і правила ранжування, може підвищувати ефективність обміну, але водночас робити виробника залежним від одного каналу збуту. Якщо умови доступу можуть бути односторонньо змінені, а накопичена репутація, клієнтські дані чи історія транзакцій не переносяться, підприємство втрачає частину власної здатності реагувати на шок. Для малого й середнього бізнесу це особливо важливо: формально незалежна фірма може фактично перетворитися на функціонально залежного учасника чужої цифрової екосистеми. Деструктивність проявляється тоді, коли рента посередника зростає саме разом із цією незамінністю, а витрати зміни каналу збуту або сервісу несуть користувачі.

Для технологічної резильєнтності ключовим є не походження технології, а можливість зберегти критичну функцію у

разі відмови, припинення постачання, кібератаки, зміни ліцензійних умов або політичного рішення в іншій юрисдикції. Це особливо важливо для енергетики, зв'язку, банків, оборонних виробництв, логістики та державних реєстрів. Тому показником стійкості має бути не максимальна частка національних компонентів, а відсутність некерованих одиничних точок відмови: наявність резерву, альтернативного маршруту, доступу до власних даних і конфігурацій, можливості заміни постачальника, внутрішніх компетенцій для аварійного режиму. Сучасні міжнародні підходи до цифрової безпеки дедалі більше виходять саме з безперервності критичних функцій, а не лише з технічного захисту окремих активів [2].

Інформаційна резильєнтність є сферою, де зв'язок між приватним стимулом і національною безпекою проявляється найбільш безпосередньо. Якщо дохід платформи залежить від кількості переглядів, тривалості взаємодії та інтенсивності реакції, алгоритмічна система отримує економічний стимул підсилувати вміст, що найкраще утримує увагу. За відсутності компенсаторних механізмів це може знижувати частку якісної інформації, збільшувати поляризацію та здешевлювати поширення неправдивого вмісту. Дж. Стігліц і М. Вентура-Болет показують, що платформи й штучний інтелект можуть одночасно підвищувати ефективність передавання інформації та погіршувати рівноважну якість інформаційного середовища, якщо економічні стимули виробництва й поширення правдивого та неправдивого вмісту залишаються неврегульованими [5].

Особливого значення ця суперечність набуває через концентрацію інфраструктури штучного інтелекту. Індекс штучного інтелекту Стенфордського університету 2026 року фіксує, що понад 90 % значущих передових моделей у 2025 р. створила приватна індустрія [11; 12]. США мають найбільшу у світі концентрацію центрів обробки даних, а виробництво найсучасніших мікросхем залишається географічно й корпоративно дуже концентрованим. Сама концентрація не доводить деструктивності. Вона стає небезпечною тоді, коли ринкова влада на одному рівні – обладнання, обчислення, базові мо-

делі чи хмарні послуги – використовується для обмеження альтернатив на іншому. Дослідження ОЕСР також наголошують, що інфраструктура штучного інтелекту характеризується високими бар'єрами входу і можливістю посилення вертикальної інтеграції [9; 10]. Для невеликих відкритих економік це означає, що питання конкуренції дедалі більше переплітається з питанням технологічної безпеки.

Тому для України коректніше говорити не про максимальну технологічну незалежність, а про керованість критичної технологічної залежності [12]. Її зміст полягає у відсутності одиничних точок відмови, наявності альтернативних постачальників або резервних режимів, технічній можливості перенесення даних, володінні критичними ключами й документацією, збереженні національних компетентностей для підтримки системи та здатності держави продовжувати виконання життєво важливих функцій за зовнішнього обмеження. Така автономія не означає автаркії. Навпаки, міжнародна спеціалізація і союзницька кооперація залишаються економічно необхідними, але мають будуватися так, щоб взаємозалежність не перетворювалася на односторонню незамінність. Світовий банк також наголошує, що країнам, які розвиваються, не обов'язково відтворювати весь технологічний ланцюг, однак простого імпорту готових рішень недостатньо без локальних даних, кадрів, адаптації та спроможності безпечно інтегрувати технології [13].

Така постановка особливо важлива, оскільки глобальні цифрові екосистеми дедалі виразніше стають елементом геоекономічної конкуренції. Європейський Союз у 2026 р. прямо пов'язав технологічну суверенність із конкурентоспроможністю, резильєнтністю та зменшенням структурних залежностей у напівпровідниках, хмарних послугах, штучному інтелекті й відкритому програмному забезпеченні. Американська політика, зі свого боку, розглядає лідерство у штучному інтелекті як складову економічної конкурентоспроможності й національної безпеки та передбачає просування за кордон комплексних американських технологічних рішень – від обладнання і моделей до програмного забезпечення та стандартів [14; 15;

16]. Для України це не аргумент на користь дистанціювання від союзників, а підстава усвідомлювати, що технологічний вибір має довгострокову інституційну й політичну траєкторію. Резильентна інтеграція означає диверсифіковану взаємозалежність із партнерами, а не безумовну прив'язаність до одного приватного або юрисдикційного центру.

У регуляторній політиці Європейського Союзу і США сформувалися різні способи відповіді на ці проблеми. Європейський підхід більшою мірою орієнтований на попереднє обмеження системної ринкової влади та ризикових практик: для найбільших цифрових посередників установлюються спеціальні обов'язки, що мають зменшувати самопідсилення ринкової влади, а для суспільно значущих цифрових і алгоритмічних систем застосовується диференціація вимог залежно від ризику [15]. Американська модель більше акцентує на швидкість інновацій, приватні інвестиції, інфраструктуру, глобальне технологічне лідерство і національну безпеку, зберігаючи значну роль загального конкурентного, споживчого, кримінального й галузевого права. Водночас

федеральні правила використання штучного інтелекту державними установами не відмовляються від захисту прав, приватності та підзвітності [16].

Ці моделі не варто спрощувати до протиставлення «жорстке регулювання» і «свобода інновацій». Вони по-різному розподіляють вагу між попередженням шкоди та нарощуванням технологічної спроможності. Для аналізу деструктивного підприємництва доцільно порівнювати їх за однаковими критеріями (табл. 3). Європейський підхід сильніший там, де проблема вже пов'язана з інфраструктурною ринковою владою, непрозорим посередництвом і високими ризиками для прав людини. Американський – там, де регуляторна мета безпосередньо поєднується з конкурентоспроможністю, обчислювальною інфраструктурою та безпековою перевагою.

Для України найважливіше не механічно поєднати два набори правил, а визначити, який інструмент змінює конкретний деструктивний стимул за найменших втрат для продуктивного підприємництва.

Таблиця 3

Підходи ЄС і США до обмеження деструктивних цифрових практик та висновки для України

Критерій	Європейський Союз	США	Висновки для України
Ринкова влада платформ	Сильніший попередній контроль системно важливих посередників і спеціальні обов'язки	Переважно загальне конкурентне право та галузеве правозастосування	Поєднати загальне конкурентне право з раннім аналізом цифрових вузьких місць
Алгоритмічні ризики	Формалізована диференціація вимог за рівнем ризику та захистом фундаментальних прав	Більш розосереджене галузеве регулювання; окремі федеральні вимоги для державного використання	Високовпливові рішення – підзвітність і людський перегляд; малоризикові – мінімальний тягар
Швидкість інновацій	Більше попередніх обов'язків, що можуть збільшувати витрати відповідності	Виразний акцент на усуненні бар'єрів, швидкому впровадженні й приватних інвестиціях	Не переносити цивільну тривалість процедур на критичні воєнні випробування
Інфраструктурна спроможність	Поєднання регулювання з розвитком спільної цифрової та обчислювальної інфраструктури	Сильний акцент на центрах обробки даних, енергетиці, мікросхемах і приватному капіталі	Нарощувати критичні обчислювальні та кадрові спроможності без автаркії
Національна безпека	Безпека інтегрується з правами, стійкістю мереж і захистом критичної інфраструктури	Безпека і технологічне лідерство є одними з центральних мотивів політики	Спеціальний швидкий, але підзвітний режим для оборонних і критичних систем

Критерій	Європейський Союз	США	Висновки для України
Витрати регулювання для малих підприємств	Ризик значного адміністративного навантаження компенсується пропорційністю окремих режимів	Менше загальних попередніх вимог, але вища невизначеність галузевого правозастосування	Диференціювати обов'язки за масштабом потенційної шкоди, а не за самим фактом використання ІІІ
Технологічна автономія	Акцент на стратегічній автономії та спільних європейських спроможностях	Акцент на національному лідерстві, інфраструктурі й експорті технологічної екосистеми	Керованість критичних залежностей, сумісність із партнерами та свобода критичного рішення

Джерело: складено за [14; 15; 16].

Ключові ризики для України та інститути їх уникнення

В українському регуляторному полі вже існують окремі елементи, здатні впливати на деструктивні цифрові практики, але вони залишаються фрагментованими. Загальне конкурентне законодавство дозволяє реагувати на зловживання ринковою владою, а Антимонопольний комітет уже застосовує його до цифрових сервісів і хмарного ринку [17; 18]. У 2026 р. Комітет, зокрема, встановив зловживання домінуючим становищем у міській цифровій платформі та, розглядаючи концентрацію у сфері хмарних послуг, виявив обмежену можливість споживачів змінювати постачальника, наклавши відповідні виконавчі приписи. Це важливий сигнал: наявні інструменти не є безсильними. Проте вони переважно реагують на вже сформовану проблему, тоді як цифрові ринки потребують також раннього виявлення вузьких місць, оцінювання витрат переходу, доступу до даних і взаємозв'язку між різними рівнями цифрової екосистеми.

Найбільш наочним прикладом є державні цифрові закупівлі. Під час війни й відбудови держава буде одним із найбільших покупців хмарних послуг, систем управління даними, алгоритмічних засобів, рішень для енергетики, транспорту, медицини, освіти та безпеки. Загальні правила закупівель передбачають конкурентні процедури і не допускають штучного звуження конкуренції [19], але для цифрової інфраструктури цього недостатньо. Дешевша ціна на момент укладення договору може приховувати високу майбутню вартість виходу: неможливість перенести дані, залежність від закритого формату, відсутність документації, прив'язку до одного постачальника оновлень або хмарних обчислень. Тому оцінювання закупівлі має включати не лише

початкову ціну, а й повну вартість життєвого циклу залежності. Саме через закупівельні вимоги держава може зробити сумісність, переносимість даних, модульність і резервування економічно вигідними характеристиками продукту.

Для воєнної України деструктивне цифрове підприємництво має кілька особливо небезпечних каналів, але їх потрібно аналізувати через конкретні економічні механізми, а не через загальний перелік усіх ризиків цифровізації (табл. 4). Перший канал – комерційна архітектура інформаційного посередництва. Російські інформаційні операції, мережі неавтентичних облікових записів, вербування або шахрайство самі по собі не є підприємницькою діяльністю платформи. Деструктивний компонент виникає там, де платформа, знаючи про системний ризик, продовжує отримувати вигоду від алгоритмічного підсилення небезпечного вмісту, прихованої реклами або непрозорих механізмів взаємодії, бо саме вони збільшують дохід. Тоді приватний стимул платформи і безпековий інтерес держави входять у прямиий конфлікт.

Другий канал – технологічне замикання критичних функцій на одному зовнішньому постачальнику. Для українського бізнесу використання іноземних хмарних, програмних або алгоритмічних сервісів часто є найбільш раціональним способом швидко підвищити продуктивність. Проблема виникає не через іноземне походження технології, а через відсутність реального виходу. Якщо дані неможливо перенести, альтернативне рішення несумісне, а постачальник має право односторонньо змінити ціну, географію доступу або умови використання, залежність стає джерелом приватної ренти й одночасно системної вразливості. Для оборонного підприємства, банку, енергетичної

компанії чи органу державної влади це вже не звичайний комерційний ризик, а питання безперервності критичної функції. Саме тут технологічна залежність переходить у поле деструктивного підприємництва.

Третій канал – високовпливові алгоритмічні рішення у фінансах, соціальній політиці та відбудові. Масове використання автоматизованого оцінювання може бути продуктивним, якщо воно скорочує час опрацювання заяв, допомагає виявляти шахрайство і зменшує адміністративні витрати. Але після війни вітчизняні дані будуть особливо неповними, – переміщене населення, знищені чи втрачені документи, дані з територій, що були під окупацією, офіцій-

на нерівномірність доходів через неформальну зайнятість створюватимуть нетипові профілі, які система може трактувати як ризикові. Якщо постачальник отримує вигоду від автоматизації, але не несе достатньої відповідальності за помилкову відмову у компенсації, кредиті, страхуванні чи соціальній підтримці, виникає класичний механізм екстерналізації ризику. Тому право на людський перегляд, перевірюваність даних і можливість оскарження є не формальною процедурою, а способом повернути частину вартості помилки тому, хто створює і продає систему.

Таблиця 4

Ключові ризики деструктивного цифрового підприємництва в Україні

Ризикова ситуація	Механізм деструктивності	Інституційна прогалина	Потенційний системний ефект	Цільова зміна політики
Залежність від глобальних платформ у торгівлі та інформаційному посередництві	Ринкова влада, інформаційна асиметрія, поведінкова експлуатація	Загальне конкурентне право діє переважно реактивно; обмежена прозорість системних ризиків	Втрата доступу до ринку, монетизація дезінформації, інформаційна вразливість	Посилення аналізу цифрових ринків, вимоги до системних ризиків і переносимості бізнес-даних
Критична функція залежить від одного хмарного або алгоритмічного постачальника	Технологічне замикання	У закупівлях і договорах не завжди враховується повна вартість виходу та безперервність	Переривання державних, оборонних або бізнес-процесів під час кризи	Вимоги до сумісності, експорту даних, резервних сценаріїв, документації та альтернативного постачальника
Автоматизовані рішення щодо кредиту, компенсації, соціальної підтримки чи страхування	Інформаційна асиметрія та екстерналізація ризику	Фрагментовані вимоги до перевірки даних, пояснення та оскарження	Закріплення вразливості, дискримінація, втрата довіри до відбудови	Людський перегляд, незалежне випробування, право оскарження, відповідальність за помилку
Військові та подвійного призначення системи штучного інтелекту	Екстерналізація ризику та технологічна непрозорість	Потреба одночасно забезпечити швидкість випробувань і персоніфіковану відповідальність	Помилки з незворотними наслідками, витік даних, залежність від зовнішньої системи	Прискорені процедури, випробування в умовах протидії, журналювання, межі автономності та довірна відповідальність
Цифрові проекти повоєнної відбудови	Регуляторний арбітраж і технологічне замикання	Терміновість закупівель може переважати вимоги до сумісності та майбутньої конкуренції	Закріплення приватного вузького місця на роки, відтік ренти й даних	Оцінка життєвого циклу залежності, модульна архітектура, права на дані й критичну документацію
Масштабна автоматизація початкових професійних функцій	Можливий зовнішній ефект, але не автоматично деструктивне підприємництво	Недостатні стимули до спільного фінансування нових траєкторій підготовки	Відкладений дефіцит досвідчених кадрів і послаблення технологічної спроможності	Співфінансування навчання, наставництва, перепідготовки та нових професійних сходиночок

Джерело: складено за [17–20].

Четвертий канал – військові та подвійного призначення системи штучного інтелекту. Тут особливо небезпечно змішувати технологію і спосіб її застосування. О. Костенко слушно наголошує, що одна й та сама система розпізнавання може використовуватися і для перехоплення ворожого безпілота, і для наведення ударної системи; отже, вирішальними є контекст, суб'єкт рішення, правила застосування і розподіл відповідальності [20]. Деструктивна підприємницька практика може виникнути, якщо розробник приховує відомі обмеження, перебільшує точність, ухиляється від випробувань у ворожому середовищі або перекладає весь ризик помилки на державного замовника, хоча саме невизначеність системи є частиною комерційної пропозиції. Війна обґрунтовує прискорення випробувань і закупівель, але не усунення відповідальності. Україна вже експериментує зі спеціальними режимами розвитку військових товарів у сфері штучного інтелекту [21], що створює можливість поєднати швидкість із чіткими умовами доступу, сумісності та перевірки.

П'ятий канал – повоєнна цифровізація відбудови. Вона створить великий і привабливий ринок для постачальників систем управління будівництвом, земельними даними, компенсаціями, логістикою, міською інфраструктурою, охороною здоров'я, освітою та енергетикою. Саме масштаб і терміновість можуть посилити регуляторний арбітраж: під гаслом швидкості замовник погоджується на закриту архітектуру, довгий строк ексклюзивної підтримки, передачу ключових даних постачальнику або відсутність технічної документації. Приватно такий контракт може бути вигідним обом сторонам у короткостроковому періоді, але суспільство отримує майбутні витрати виходу, обмеження конкуренції і зовнішню залежність. Отже, у відбудові деструктивність може формуватися не через «погану технологію», а через контрактну архітектуру, яка робить незамінність постачальника джерелом майбутнього прибутку.

Напрями державної політики уникнення ризиків деструктивного цифрового підприємництва

З таблиці 4 слідує, що для України не потрібен окремий орган для регулювання

деструктивного підприємництва. Необхідно змінити логіку роботи вже існуючих інститутів так, щоб вони бачили не лише формальне порушення норми, а й механізм накопичення системної шкоди. Антимонопольне регулювання має оцінювати не лише ціну та частку ринку, а й контроль над даними, витрати переходу і вертикальне замикання. Захист персональних даних повинен враховувати не тільки правову підставу обробки, а й економічний стимул до надмірного накопичення. Кібербезпекова політика має оцінювати безперервність і залежність від одного постачальника. Державний замовник – майбутню вартість виходу з цифрової системи. Галузеві регулятори – можливість алгоритмічної помилки у високо-впливових рішеннях. Такий міжсекторальний підхід не розмиває відповідальність, якщо кожному органу поставити конкретну функцію у спільному ланцюгу ризику.

З огляду на це перший системний напрям політики має полягати у підтриманні конкуренції й запобіганні перетворенню цифрового посередництва на приватне вузьке місце. Для системно важливих платформ та інфраструктурних постачальників ключовими є можливість переходу, переносимість даних, заборона штучного пов'язування критичної послуги з непотрібними додатковими сервісами, контроль практик надання переваг власним продуктам і підвищена увага до концентрацій, які можуть ліквідувати майбутню конкуренцію. Для України важливо не копіювати весь європейський адміністративний апарат, а нарощувати технічну спроможність Антимонопольного комітету аналізувати цифрові екосистеми, взаємозалежність ринків і роль даних.

Другий напрям – алгоритмічна підзвітність і захист людини там, де рішення має істотні правові, економічні або соціальні наслідки. Метою не має бути вимога розкрити весь програмний код чи пояснити кожен внутрішній операційний складний елемент моделі. Важливіше забезпечити перевірюваність результатів, документування даних і мети використання, незалежне випробування, журналювання ключових подій, можливість встановити причинний зв'язок після інциденту та право на ефективний перегляд рішення людиною. Індекс штучного інтелекту

Стенфордського університету 2026 року фіксує, що кількість задокументованих інцидентів зі штучним інтелектом зростає, а прозорість провідних розробників щодо даних, обчислювальних ресурсів і наслідків після розгортання залишається недостатньою [22]. У такому середовищі економічна перевага не повинна виникати з неможливості перевірити шкоду.

Третій напрям – технологічна резильєнтність і керованість критичних залежностей. Для державних органів, оборонних підприємств, банків, енергетики, зв'язку, транспорту і великих систем відбудови мають бути обов'язковими карти критичних залежностей, резервні сценарії, сумісні формати, можливість експорту даних, договірно визначені строки й умови припинення послуги, тестування роботи у деградованому режимі та документована процедура переходу до альтернативного постачальника. Відкритість і переносимість при цьому не можуть бути абсолютними: для оборонних і критичних даних вони мають поєднуватися з обмежуванням доступу, криптографічним захистом і спеціальними режимами зберігання. Отже, суперечність між автономією і безпекою розв'язується не відмовою від сумісності, а її контрольованою реалізацією. Світовий банк формулює близький підхід як необхідність вбудовувати довіру та безпеку у цифрові системи ще на етапі проєктування [23].

Четвертий напрям – інформаційна, кібернетична й оборонна безпека, зорієнтована на економічні стимули. У сфері інформаційних платформ держава не повинна регулювати «правильність думки», але має вимагати управління системними ризиками, прозорості суспільно значущої реклами, протидії координованій неавтентичній поведінці та можливості незалежного дослідження агрегованих даних про поширення небезпечного вмісту. У кіберсфері необхідно створювати для постачальників стимули інвестувати у безпеку продукту протягом його життєвого циклу, а не перекладати вартість вразливостей на користувача. В оборонних застосуваннях регулювання має бути ризик-орієнтованим і функціональним: швидке випробування і закупівля мають поєднуватися з перевіркою в умовах нав-

мисної протидії, чіткими межами автономності, журналами критичних рішень та персоніфікованою відповідальністю. Воєнна необхідність може змінювати допустимий рівень ризику, але не повинна усувати сам принцип відповідальності.

П'ятий напрям – суспільна віддача від цифровізації, державної підтримки та відбудови. Якщо держава фінансує дослідження, обчислювальну інфраструктуру, випробувальні полігони або гарантує попит через великі закупівлі, умови підтримки мають запобігати перетворенню суспільного ризику на приватну незамінність. Практичними інструментами можуть бути права держави на використання результатів у критичних цілях, вимоги до сумісності, збереження ключової документації, доступ українських виробників до створених за публічні кошти інфраструктурних ресурсів, зобов'язання щодо кібербезпеки, підготовки кадрів та підтримки продукту в кризових умовах. Там, де автоматизація створює довгостроковий ризик дефіциту компетентностей, частину приросту продуктивності доцільно спрямовувати на перепідготовку і нові траєкторії професійного становлення. Це не покарання за інновацію, а спосіб зменшити зовнішні витрати, які інакше оплачуватиме суспільство.

Особливого значення набуває узгодженість цих політик. Якщо конкурентна політика вимагає переносимості даних, а безпекова – їх обмеженого поширення, рішення повинно залежати від критичності функції та категорії даних. Якщо швидкість оборонної інновації конфліктує з попередньою перевіркою, доцільні прискорені випробування й поетапне нарощування автономності замість відмови від підзвітності. Якщо розвиток національної спроможності дорожчий за імпорт, питання має вирішуватися через ціну потенційного переривання критичної функції, а не лише через поточну закупівельну ціну. Такий підхід відповідає логіці пропорційного управління ризиком: не все в цифровій економіці повинно мати однаковий рівень резервування і контролю, але для системно важливих функцій допустимий рівень залежності має бути нижчим, ніж для звичайних комерційних сервісів [24].

Для практичного виявлення деструктивної цифрової бізнес-моделі доцільно використовувати простий аналітичний тест. Регулятор, державний замовник або великий корпоративний клієнт мають з'ясувати: чи зростає дохід постачальника разом із залежністю користувача; чи має користувач реальну можливість перейти до альтернативи без непропорційних втрат; чи створює бізнес-практика шкоду, яку оплачує третя сторона; чи може постраждалий перевірити й оскаржити результат; чи несе постачальник частину витрат у разі помилки або зловживання; чи зберігається критична функція під час зовнішнього обмеження. Негативна відповідь на кілька таких питань ще не є доказом деструктивності, але сигналізує про необхідність поглибленої оцінки. Перевага такого тесту полягає в тому, що він концентрується на економічному механізмі, а не на ярлику «небезпечна технологія».

Звідси випливає і більш точне розуміння цифрової незалежності України. Вона не має вимірюватися часткою національного походження кожного компонента і не повинна перетворюватися на політику технологічної самоізоляції. Її зміст – у збереженні свободи критичного рішення. Людина повинна мати можливість оскаржити важливий алгоритмічний висновок; підприємство – змінити платформу чи постачальника без втрати власних даних і ринку; держава – зберегти контроль над критичними даними та продовжити надання життєво важливих послуг; оборонна система – функціонувати за втрати окремого зовнішнього сервісу. Саме така керована взаємозалежність є економічно реалістичним змістом технологічної автономії під час війни і відбудови.

Висновки. Проведений аналіз дає підстави уточнити саму природу деструктивного цифрового підприємництва. Його не можна визначати ані за технологічною новизною, ані за наявністю будь-якого негативного наслідку, ані за іноземним походженням цифрового продукту. Деструктивність є характеристикою структури економічного стимулу: приватна дохідність систематично залежить від створення, посилення або перенесення на суспільство істотної шкоди, а суб'єкт має можливість не нести її повної вартості. Цифрове середовище ро-

бити цей механізм особливо небезпечним, оскільки мережеві ефекти, контроль даних, алгоритмічне посередництво, масштабованість програмних рішень і високі витрати переходу дозволяють одночасно збільшувати приватну ренту та поширювати зовнішній ефект на великі групи користувачів, ринки й навіть державні системи.

Розгляд деструктивного підприємництва крізь призму резильєнтності дозволяє виявити наслідок, який не видно з традиційного аналізу ефективності. Бізнес-модель може бути дешевою, інноваційною і зручною, але поступово зменшувати кількість альтернатив, резервів, компетенцій і каналів відновлення. Саме в цьому полягає розрив між приватною ефективністю і суспільною стійкістю. Економічна деструктивність проявляється у перетворенні посередницької влади на ренту й залежність підприємств; технологічна – у замиканні критичних функцій на незамінних постачальниках і закритих технологічних комплексах; соціальна – в комерційному використанні нерівності, поведінкової вразливості та інформаційної асиметрії; інформаційна – у такій економіці уваги, за якої неправдивий, поляризуючий або маніпулятивний вміст може мати вищу приватну дохідність, ніж суспільно корисна інформація.

Для України ключовим є наскрізний вимір зовнішньої залежності. Міжнародна спеціалізація і використання передових іноземних технологій є необхідними для воєнної економіки та відбудови. Небезпека виникає тоді, коли взаємозалежність стає асиметричною: критична функція не має резерву; дані неможливо перенести; постачальника практично неможливо замінити; власні фахівці не здатні підтримати систему; або доступ до технології залежить від зовнішнього рішення, яке Україна не може передбачити чи компенсувати. Деструктивне підприємництво здатне поглиблювати таку залежність, якщо постачальник свідомо робить незамінність джерелом ренти. Тому технологічна автономія України не повинна означати самоізоляцію. Її практичний зміст – керованість критичних залежностей, диверсифікація, резервування та збереження свободи критичного рішення.

Відповідно, метою державної політики має бути не максимальне регулювання цифрової сфери, а формування такого інституційного середовища, в якому прибутковість бізнесу узгоджується зі стійкістю суспільства. Практичним критерієм якості політики є те, чи зменшує вона можливість заробляти на незамінності, непрозорості, поведінковій вразливості та перенесенні ризику; чи зберігає конкуренцію і можливість виходу; чи підтримує резерви, людські компетенції й достовірне інформаційне середовище; чи не створює непропорційного тягаря для продуктивних інновацій. За такого підходу резильєнтність стає не додатковою темою поряд із регулюванням деструктивного підприємництва, а інтегральним критерієм оцінки його суспільної безпеки та результативності державної відповіді.

Література

1. Baumol W. J. Entrepreneurship: Productive, Unproductive, and Destructive. *Journal of Political Economy*. 1990. Vol. 98, No. 5, Part 1. Pp. 893-921. DOI: 10.1086/261712.
2. OECD. Economic Security in a Changing World. Paris : OECD Publishing, 2025. Ch. 6. URL: https://www.oecd.org/en/publications/2025/09/economic-security-in-a-changing-world_78f3b129/full-report/building-stronger-defences-for-a-digital-future-the-role-of-cybersecurity_484bcb90.html
3. Naudé W. Destructive Digital Entrepreneurship. *IZA Discussion Paper*. 2023. No. 16483. 56 p. URL: <https://docs.iza.org/dp16483.pdf>
4. Allcott H., Gentzkow M., Song L. Digital Addiction. *American Economic Review*. 2022. Vol. 112, No. 7. Pp. 2424-2463. DOI: 10.1257/aer.20210867.
5. Stiglitz J.E., Ventura-Bolet M. The Impact of AI and Digital Platforms on the Information Ecosystem. *NBER Working Paper*. 2025. No. 34318. DOI: 10.3386/w34318.
6. Orben A., Meier A., Dalglish T., Blakemore S.-J. Mechanisms Linking Social Media Use to Adolescent Mental Health Vulnerability. *Nature Reviews Psychology*. 2024. Vol. 3. Pp. 407-423. DOI: 10.1038/s44159-024-00307-y.
7. Brynjolfsson E., Li D., Raymond L. Generative AI at Work. *The Quarterly Journal of Economics*. 2025. Vol. 140, No. 2. Pp. 889-942. DOI: 10.1093/qje/qjae044.
8. Hyman B.G., Lahey B., Ni K., Pilossoph L. How Retractable are AI-Exposed Workers? *NBER Working Paper*. 2025. No. 34174. Revised May 2026. DOI: 10.3386/w34174.
9. OECD. Competition in the Age of AI: Initial Evidence from Microdata. *OECD Artificial Intelligence Papers*. 2026. No. 64. DOI: 10.1787/6f88a1ea-en.
10. OECD. Competition in Artificial Intelligence Infrastructure. *OECD Roundtables on Competition Policy Papers*. 2025. No. 330. DOI: 10.1787/623d1874-en.
11. Stanford Institute for Human-Centered Artificial Intelligence. *AI Index Report 2026*. Stanford University, 2026. URL: https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf
12. Костенко О. Як штучний інтелект змінює уявлення про незалежність держав: що показав Stanford AI Index 2026. *ZN.UA*. 22.08.2026. URL: <https://zn.ua/ukr/TECHNOLOGIES/jak-shtuchnij-intelekt-zminjuje-ujavlennja-pro-nezalezhnist-derzhav-shcho-pokazav-stanford-ai-index-2026.html>
13. World Bank. *World Development Report 2026: The Promise of Artificial Intelligence*. Washington, DC : World Bank, 2026. URL: <https://www.worldbank.org/en/publication/wdr2026>
14. European Commission. Communication on European Tech Sovereignty, accompanied by an EU Open Source Strategy. COM(2026) 503. 03.06.2026. URL: <https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy>
15. Regulation (EU) 2022/2065 on a Single Market for Digital Services; Regulation (EU) 2022/1925 on contestable and fair markets in the digital sector; Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence. URL: <https://eur-lex.europa.eu>
16. The White House. Winning the AI Race: America's AI Action Plan. 23.07.2025. URL: <https://www.whitehouse.gov/releases/2025/07/white-house-unveils-americas-ai-action-plan/>
17. Про захист економічної конкуренції : Закон України від 11.01.2001 № 2210-III. URL: <https://zakon.rada.gov.ua/laws/show/2210-14>
18. Антимонопольний комітет України. АМКУ дозволив ПрАТ «Київстар» набуті контроль над ТОВ «ГІГАКЛІАУД» за умови виконання зобов'язань. URL: <https://amcu.gov.ua/news/amku-dozvoliv-prat-kyivstar-nabuty-kontrol-nad-tov-hihaklaud-za-umovy-vikonannia-zoboviazan>
19. Про публічні закупівлі : Закон України від 27.05.2026 № 4888-IX. URL: <https://zakon.rada.gov.ua/laws/show/4888-20>
20. Костенко О. Щит має бути дешевшим за меч: як війна змінює філософію штучного інтелекту. *ZN.UA*. 06.08.2026. URL: <https://zn.ua/ukr/TECHNOLOGIES/shchit-maje-buti-deshevshim-za-mech-jak-vijna-zminjuje-filosofiju-shtuchnoho-intelektu.html>
21. Деякі питання реалізації експериментального проекту щодо розвитку товарів військового призначення у сфері технологій штучного інтелекту. : постанова Кабінету Міністрів України від 12.03.2026 № 310. URL: <https://zakon.rada.gov.ua/laws/show/310-2026-%D0%BF>
22. Stanford Institute for Human-Centered Artificial Intelligence. *AI Index Report 2026. Chapter 3: Responsible AI*. Stanford University, 2026. URL: <https://hai.stanford.edu/ai-index/2026-ai-index-report/responsible-ai>
23. World Bank. Trust by Design: Securing Digital Development. 09.06.2026. URL:

<https://www.worldbank.org/en/results/2026/06/09/trust-by-design-securing-digital-development>

24. OECD. *OECD Digital Economy Outlook 2024. Vol. 2: Strengthening Connectivity, Innovation and Trust*. Paris : OECD Publishing, 2024. DOI: 10.1787/3adf705b-en.

References

1. Baumol, W.J. (1990). Entrepreneurship: Productive, unproductive, and destructive. *Journal of Political Economy*, 98(5), Part 1, 893-921. <https://doi.org/10.1086/261712>

2. OECD. (2025). *Economic security in a changing world* (Chapter 6: Building stronger defences for a digital future). OECD Publishing. Retrieved from https://www.oecd.org/en/publications/2025/09/economic-security-in-a-changing-world_78f3b129/full-report/building-stronger-defences-for-a-digital-future-the-role-of-cybersecurity_484bcb90.html

3. Naudé, W. (2023). Destructive digital entrepreneurship. IZA Discussion Paper, 16483. <https://docs.iza.org/dp16483.pdf>

4. Allcott, H., Gentzkow, M., & Song, L. (2022). Digital addiction. *American Economic Review*, 112(7), 2424-2463. <https://doi.org/10.1257/aer.20210867>

5. Stiglitz, J. E., & Ventura-Bolet, M. (2025). The impact of AI and digital platforms on the information ecosystem. NBER Working Paper, 34318. <https://doi.org/10.3386/w34318>

6. Orben, A., Meier, A., Dalgleish, T., & Blake-more, S.-J. (2024). Mechanisms linking social media use to adolescent mental health vulnerability. *Nature Reviews Psychology*, (3), 407-423. <https://doi.org/10.1038/s44159-024-00307-y>

7. Brynjolfsson, E., Li, D., & Raymond, L. (2025). Generative AI at work. *The Quarterly Journal of Economics*, 140(2), 889-942. <https://doi.org/10.1093/qje/qjae044>

8. Hyman, B. G., Lahey, B., Ni, K., & Pilossoph, L. (2025). How retrainable are AI-exposed workers? NBER Working Paper, 34174 (rev. May 2026). <https://doi.org/10.3386/w34174>

9. OECD. (2026). Competition in the age of AI: Initial evidence from microdata. *OECD Artificial Intelligence Papers*, 64. <https://doi.org/10.1787/6f88a1ea-en>

10. OECD. (2025). Competition in artificial intelligence infrastructure. *OECD Roundtables on Competition Policy Papers*, 330. <https://doi.org/10.1787/623d1874-en>

11. Stanford Institute for Human-Centered Artificial Intelligence. (2026). *AI Index Report 2026*. Stanford University. Retrieved from https://hai.stanford.edu/assets/files/ai_index_report_2026.pdf

12. Kostenko, O. (2026, August 22). Yak shtuchnyi intelekt zminiue uiavlennia pro nezalezhnist derzhav: shcho pokazav Stanford AI Index 2026. ZN.UA. Retrieved from <https://zn.ua/ukr/TECHNOLOGIES/jak-shtuchnij-intelekt-zminjuje-ujavlennja-pro-nezalezhnist-derzhav-shcho-pokazav-stanford-ai-index-2026.html>

<https://www.worldbank.org/en/results/2026/06/09/trust-by-design-securing-digital-development>

13. World Bank. (2026). *World Development Report 2026: The promise of artificial intelligence*. Retrieved from <https://www.worldbank.org/en/publication/wdr2026>

14. European Commission. (2026, June 3). *Communication on European tech sovereignty, accompanied by an EU Open Source Strategy* (COM(2026) 503). Retrieved from <https://digital-strategy.ec.europa.eu/en/library/communication-european-tech-sovereignty-accompanied-eu-open-source-strategy>

15. European Parliament and Council of the European Union. (2022–2024). Digital Services Act (EU) 2022/2065; Digital Markets Act (EU) 2022/1925; Artificial Intelligence Act (EU) 2024/1689. Retrieved from <https://eur-lex.europa.eu>

16. The White House. (2025, July 23). *Winning the AI race: America's AI Action Plan*. Retrieved from <https://www.whitehouse.gov/releases/2025/07/white-house-unveils-americas-ai-action-plan/>

17. Verkhovna Rada of Ukraine. (2001). Pro zakhyst ekonomichnoi konkurentsii. (Law No. 2210-III) Retrieved from <https://zakon.rada.gov.ua/laws/show/2210-14>

18. Antymonopolnyi komitet Ukrainy. (2026). AMKU dozvoliv PrAT «Kyivstar» nabuty kontrol nad TOV «HIHAKLAUD» za umovy vykonannia zobov'язan. Retrieved from <https://amcu.gov.ua/news/amku-dozvoliv-prat-kyivstar-nabuty-kontrol-nad-tov-hihaklaud-za-umovy-vykonannia-zobov'язan>

19. Verkhovna Rada of Ukraine. (2026). Pro publichni zakupivli [On public procurement] (Law No. 4888-IX). <https://zakon.rada.gov.ua/laws/show/4888-20>

20. Kostenko, O. (2026, August 6). Shchyt maie buty deshevshym za mezh: yak viina zminiue filosofiiu shtuchnoho. ZN.UA. Retrieved from <https://zn.ua/ukr/TECHNOLOGIES/shchyt-maje-buty-deshevshim-za-mech-jak-vijna-zminjuje-filosofiju-shtuchnoho-intelektu.html>

21. Cabinet of Ministers of Ukraine. (2026). Dei-aki pytannia realizatsii eksperymentalnoho proektu shchodo rozvytku tovariv viiskovoho pryznachennia u sferi tekhnolohii shtuchnoho intelektu. (Resolution No. 310). Retrieved from <https://zakon.rada.gov.ua/laws/show/310-2026-%D0%BF>

22. Stanford Institute for Human-Centered Artificial Intelligence. (2026). *AI Index Report 2026: Responsible AI*. Stanford University. Retrieved from <https://hai.stanford.edu/ai-index/2026-ai-index-report/responsible-ai>

23. World Bank. (2026, June 9). Trust by design: Securing digital development. Retrieved from <https://www.worldbank.org/en/results/2026/06/09/trust-by-design-securing-digital-development>

24. OECD. (2024). *OECD Digital Economy Outlook 2024: Strengthening connectivity, innovation and trust* (Vol. 2). OECD Publishing. <https://doi.org/10.1787/3adf705b-en>

ЕКОНОМІКА ТА МІЖНАРОДНІ ЕКОНОМІЧНІ ВІДНОСИНИ (ЗА СПЕЦІАЛІЗАЦІЄЮ)
DESTRUCTIVE DIGITAL ENTREPRENEURSHIP IN SHAPING THE SYSTEMIC
VULNERABILITY OF UKRAINE'S ECONOMY: CHALLENGES TO RESILIENCE
AND DEVELOPMENT SECURITY

Yu. V. Kindzerskyi, D.E., Department of Innovation Policy, Economy and Organization of High Technologies, Institute for Economics and Forecasting of the NAS of Ukraine

Methods. The institutional, systemic and comparative approaches, causal analysis and analytical typology are applied. Destructiveness is assessed through the structure of private incentives, the externalisation of social harm and the ability of a digital business model to create systemic indispensability. Resilience is considered as the capacity of the economy, society and the state to preserve critical functions, adapt and recover after a shock.

Results. The meaning of destructive digital entrepreneurship is specified and distinguished from technological risk, digital divides, criminal activity and external dependence as such. The mechanisms of market power, information asymmetry, behavioural exploitation, risk externalisation, regulatory arbitrage and technological lock-in are systematised. Their effects on economic, technological, social and informational resilience are disclosed. EU and US approaches are compared, and the risks that are critical for Ukraine during the war and post-war digital reconstruction are identified. Private efficiency does not guarantee resilience when lower costs are accompanied by fewer alternatives, reserves and key recovery channels. The boundary between manageable interdependence and supplier indispensability is defined.

Novelty. A cross-cutting causal framework is proposed: private incentive generates a business practice; the practice produces a negative externality; its concentration in a critical function creates systemic vulnerability and reduces resilience. Ukraine's digital autonomy is substantiated not as autarky, but as the manageability of critical dependencies and preservation of the freedom of critical decision-making.

Practical value. Guidelines are formulated for competition, procurement, innovation, social, information and security policies. A diagnostic test for regulators and public purchasers is proposed. It focuses on supplier indispensability, data portability, contestability of high-impact decisions, allocation of error costs, redundancy and continuity of critical functions.

Keywords: destructive entrepreneurship, digital business models, resilience, systemic vulnerability, national security, technological dependence, digital platforms, artificial intelligence, government regulation, post-war reconstruction.

Стаття надійшла до редакції 25.08.2026 р.

Прийнята до публікації 10.09.2026 р.

Дата публікації 30.09.2026 р.