

УДК 321.01:004.738.5

DOI [https://doi.org/10.32689/2523-4625-2025-2\(78\)-1](https://doi.org/10.32689/2523-4625-2025-2(78)-1)

Олег АГАРКОВ

доктор політичних наук, професор, завідувач кафедри соціальної роботи,
Карпатський інститут підприємництва
Відкритого міжнародного університету розвитку людини «Україна»,
agarkov.oleg1980@gmail.com
ORCID: 0000-0002-0735-3226

Григорій БУКАНОВ

доктор наук з державного управління, професор, професор кафедри конституційного,
адміністративного та трудового права,
Національний університет «Запорізька політехніка»,
vip.gregorov5@gmail.com
ORCID: 0000-0002-5398-5953

УКРАЇНА В УМОВАХ ЦИФРОВОГО НЕОФЕОДАЛІЗМУ

Стаття присвячена аналізу впливу цифрового неофеодалізму на політичні та соціально-економічні процеси в Україні. Застосовуючи методологію, яка включає концептуалізацію і SWOT-аналіз, в дослідженні ідентифікуються прояви цифрового неофеодалізму в Україні.

Цифровий неофеодалізм визначається як система, що характеризується монополізацією даних, ренто-орієнтованою економікою платформ і мережевою владою, створюючи залежності, подібні до феодальних. В Україні соціальна реальність формує бінарність, де швидка цифровізація співіснує з російською агресією. Такий стан речей, з одної сторони, становить загрозу втрати Україною суверенітету, але з іншої сторони також відкриває можливості для розвитку національних екосистем.

За допомогою SWOT-аналізу розкриті сильні сторони України в умовах цифрового неофеодалізму, такі як IT-сектор і «Дія», які у поєднанні з можливостями (GDPR, 5G), створюють потенціал для цифрової екосистеми, тоді як слабкі сторони (цифровий розрив, залежність від хмарних сервісів) і загрози (кібератаки, дезінформація) формують ризик цифрової ізоляції.

На основі SWOT-аналізу пропонуються стратегічні рекомендації, а саме локалізація даних і розвиток національних платформ, інтегрованих із «Дією», для зменшення залежності від технічних гігантів; інвестиції в 5G-мережі та цифрову освіту для усунення цифрового розриву; розробка національного стандарту захисту даних і інтеграція GDPR для обмеження впливу платформ; посилення співпраці з ЄС, НАТО та нейтральними країнами для залучення ресурсів; розвиток відкритих технологічних екосистем для демократизації цифрового простору.

Ключові слова: цифровий неофеодалізм, мережева влада, колоніалізм даних, цифровий суверенітет, кібербезпека, цифровий розрив, дезінформація, економічна залежність, національні екосистеми, інклюзивний розвиток, локалізація даних.

Oleh Aharkov, Hryhorii Bukanov. UKRAINE IN THE CONDITIONS OF DIGITAL NEOFEUDALISM

The article is dedicated to analyzing the impact of digital neo-feudalism on political and socio-economic processes in Ukraine. Employing a methodology that includes conceptualization and SWOT analysis, the study identifies manifestations of digital neo-feudalism in Ukraine.

Digital neo-feudalism is defined as a system characterized by data monopolization, a rent-oriented platform economy, and networked power, creating dependencies akin to feudal ones. In Ukraine, the social reality forms a duality where rapid digitalization coexists with Russian aggression. This situation, on the one hand, poses a threat to Ukraine's sovereignty but, on the other, opens opportunities for developing national ecosystems.

Through SWOT analysis, the study highlights Ukraine's strengths in the context of digital neo-feudalism, such as its IT sector and the "Diia" platform, which, combined with opportunities (GDPR, 5G), create potential for a digital ecosystem. Meanwhile, weaknesses (digital divide, dependence on cloud services) and threats (cyberattacks, disinformation) pose risks of digital isolation.

Based on the SWOT analysis, strategic recommendations are proposed, including data localization and the development of national platforms integrated with «Diia» to reduce dependence on tech giants; investments in 5G networks and digital education to bridge the digital divide; development of a national data protection standard and GDPR integration to limit platform influence; strengthening cooperation with the EU, NATO, and neutral countries to attract resources; and fostering open technological ecosystems to democratize the digital space.

Key words: digital neo-feudalism, networked power, data colonialism, digital sovereignty, cybersecurity, digital divide, disinformation, economic dependency, national ecosystems, inclusive development, data localization.

Постановка проблеми. Актуальність теми зумовлена глибинними трансформаціями, які формують сучасну соціально-політичну реальність у глобальному та національному вимірах. Стрімкий розвиток цифрових технологій, концентрація інформаційних ресурсів в руках технологічних гігантів і трансформація структур влади створюють нову парадигму, що нагадує феодальні відносини. Цей феномен, який Н. Срнічек називає платформним капіталізмом [14], а Я. Бреммер – технополіарним порядком, який характеризується монополізацією даних, алгоритмічним управлінням і формуванням цифрових «феодів», де технологічні компанії виступають новими центрами влади, а користувачі стають залежними суб'єктами [1]. Для України, яка перебуває на перетині геополітичних і технологічних викликів, аналіз цифрового неофеодалізму набуває критичного значення, поєднуючи питання національної безпеки, економічного розвитку, соціальної справедливості та культурної ідентичності.

Україна, з одного боку, активно розвиває власну цифрову інфраструктуру, зокрема через проєкт «Дія», демонструючи амбіції до цифрового суверенітету. З іншого боку, вона стикається з викликами суверенітету від іноземних платформ, які домінують у глобальному інформаційному та економічному просторі. У контексті російсько-української війни, що триває з 2014 року, ця залежність створює ризики для кібербезпеки, посилюючи вразливість перед дезінформацією та кібератаками. Теоретичне осмислення цифрового неофеодалізму через призму мережевої влади М. Кастельса дозволяє зрозуміти, як глобальні платформи формують інформаційні наративи, впливаючи на суспільну думку та політичні процеси в Україні [2]. Водночас постколоніальна перспектива розкриває цифровий неофеодалізм як форму сучасного «цифрового колоніалізму», коли дані українських користувачів експлуатуються глобальними корпораціями, а держава має обмежений контроль над власним цифровим простором.

Економічний вимір проблеми не менш важливий. Платформна економіка, що є проявом цифрового неофеодалізму, трансформує ринок праці в Україні, де фріланс-платформи відіграють значну роль у працевлаштуванні ІТ-спеціалістів, але водночас посилюють залежність від іноземних посередників, які диктують умови та отримують значну частину прибутку. Концепція цифрового екстрактивізму, запропонована Н. Коулдрі і У. Мехіасом, допомагає проаналізувати, як глобальні платформи витягають економічну цінність із локальних ринків, що вимагає від України стратегій для розвитку власних цифрових екосистем [3]. Крім того,

цифровий розрив, що проявляється в обмеженому доступі до швидкісного інтернету для значної частини населення, посилює соціальну нерівність, обмежуючи можливості для освіти, працевлаштування та участі в економіці знань.

Таким чином, дослідження цифрового неофеодалізму в українському контексті є науково актуальним, оскільки дозволяє поєднати глобальні теоретичні рамки – цифровий капіталізм, мережеву владу, постколоніалізм – із практичними викликами, що стоять перед Україною. Воно сприяє розробці стратегій цифрової трансформації, які враховують національні інтереси, зміцнюють кібербезпеку, зменшують соціальну нерівність і підтримують економічну автономію. У контексті війни, геополітичних трансформацій і швидкої цифровізації, аналіз цієї теми є важливим для формування стійкої, інклюзивної та суверенної цифрової політики України.

Аналіз останніх досліджень і публікацій. Сучасний капіталізм зазнає трансформації, яку дослідники, такі як Н. Срнічек [14], Я. Бреммер [1], Мануель Кастельс [2], Нік Коулдрі та Улісес Алі Мехіас [3], Джоді Дін [4], С. Дюран [5], Й. Гал та А. Гал [6], Остен Гстрейн і Діма Коченов [7], Ярон Єнсен [8], Джоел Коткін [9], Софія Луїс [10], Кірон Пателіс [11], Анна Полін [12], Тімоті Райтц [13], Ельшад Тагізаде та Ельхан Ахмадов [15], Д. Волленберг [16], Дж. Ян [17] і Мілан Зафіровскі [18], аналізують через концепції платформного капіталізму та цифрового неофеодалізму. Ці автори описують, як концентрація економічної, інформаційної та політичної влади в руках технологічних гігантів створює нові форми залежності, нерівності та контролю, що мають паралелі з феодальними структурами. Для України, яка перебуває в умовах російсько-української війни, економічної вразливості та викликів цифрового суверенітету, ці ідеї є критично важливими.

Н. Срнічек [14] стверджує, що платформний капіталізм, втілений у діяльності компаній, таких як Google, Facebook, Uber і Airbnb, трансформує капіталістичні структури, створюючи монополістичні інфраструктури, які забезпечують взаємодію між користувачами, рекламодавцями та постачальниками послуг. Ці платформи, за Н. Срнічком, концентрують економічну та інформаційну владу, формуючи залежність, подібну до феодальних відносин, де користувачі віддають дані в обмін на доступ до сервісів, а платформи виступають цифровими «сеньйорами». Ця ідея знаходить продовження в концепції «колоніалізму даних» Н. Коулдрі та У. Мехіаса [3], які порівнюють витягання даних із користувачів із історичним привласненням ресурсів. Вони підкреслюють, що дані стають новим ресурсом, який експлуатується, створю-

ючи асиметричні відносини влади, що нагадують феодальні. Для України залежність від іноземних платформ, таких як Meta чи Google, загрожує цифровому суверенітету, оскільки контроль над даними може впливати на інформаційну безпеку, особливо в умовах гібридної війни, де дезінформація є ключовим інструментом.

На більш глибокому рівні проблему аналізує М. Кастельс [2], який у теорії мережевої влади описує, як цифрові технології, зокрема соціальні мережі, трансформують владні відносини. Масова самокомунікація створює простір для політичних і соціальних рухів, але водночас посилює контроль з боку корпорацій і держав. В Україні соціальні мережі сприяють протидії російській пропаганді, але алгоритми платформ можуть сприяти маніпуляціям, якщо не враховує локальний контекст. Ця думка перегукується з ідеєю Я. Бреммера [1], який аналізує зростання популізму та націоналізму як реакцію на нерівність, спричинену концентрацією ресурсів у руках еліт. Я. Бреммер зазначає, що розчарування громадян урядами, які не забезпечують безпеку, призводить до створення «цифрових стін» для захисту інформаційного простору. Для України це актуалізує необхідність посилення інформаційної безпеки, особливо в умовах війни, коли глобальні платформи впливають на суспільну думку.

Концепція неофеодалізму, розвинута Дж. Дін [4], Дж. Коткіним [9] і С. Дюран [5], підкреслює повернення до ієрархічних структур. Дж. Дін [4] акцентує увагу на ролі ренти та боргу, які витісняють традиційні капіталістичні механізми, створюючи нові форми експропріації. Цю ідею доповнює С. Луїс [10], яка порівнює цифрові підписки з феодальною рентою, де користувачі платять за доступ до сервісів, не володіючи ними. Дж. Коткін [9] описує нову класову структуру, де технологічні олігархи та «клерикальна еліта» (експерти, медіа) домінують над суспільством, що нагадує феодальні ієрархії. Для України це актуалізує проблему цифрового розриву, де нерівний доступ до технологій поглиблює соціальну нерівність. Т. Райтц [13] додає, що ієрархія в академічному середовищі сприяє привласненню знань, що в українському контексті посилює освітню нерівність через обмежений доступ до ресурсів.

Е. Тагізаде та Е. Ахмадов [15] аналізують технофеодалізм як глобальну боротьбу за контроль над цифровою інфраструктурою, зокрема між США та Китаєм. Для України це створює дилему, яка полягає в тому, що залежність від американських платформ, таких як Google чи Microsoft, обмежує цифровий суверенітет, тоді як китайські технології, як Huawei, викликають занепокоєння

щодо безпеки. А. Полін [12] попереджає про небезпеку «чорних скриньок» у розумних містах, які можуть призвести до неофеодальних монополій, і пропонує розвивати відкриті технологічні екосистеми для демократичного контролю. Ця ідея перегукується з аналізом Д. Волленберга [16], який розглядає неофеодалізм як ліву критику капіталізму, що відкриває можливості для альтернативних моделей, таких як децентралізовані платформи. В Україні це може означати підтримку національних цифрових екосистем для зменшення залежності від глобальних гігантів.

О. Гстрейн і Д. Коченов [7] підкреслюють ризики цифрової ідентичності, яка може посилити контроль і нерівність, що є актуальним для України в контексті впровадження цифрових паспортів і державних сервісів. Я. Єнсен [8] порівнює сучасний контроль інформації з феодальними принципами, вказуючи на співпрацю між державами та корпораціями, що має значення для аналізу кібербезпеки в Україні. М. Зафіровські [18] і К. Пателіс [11] додають культурно-політичний вимір. М. Зафіровські порівнює американський консерватизм із феодальними структурами, а К. Пателіс інтерпретує неофеодалізм як неоромантичний проєкт, що відображає ностальгію за ієрархіями, як у русі СІРІЗА в Греції. Ці ідеї допомагають розглянути цифровий неофеодалізм у ширшому контексті. Й. Гал і А. Гал аналізують небажання працівників знань ділитися інформацією, порівнюючи це з феодальною лояльністю, що актуально для розуміння цифрового розриву в Україні [6]. Дж. Ян, у свою чергу, інтерпретує технофеодалізм як продовження капіталістичних стратегій, а не новий порядок, що підкреслює необхідність критичного підходу до цифрових трансформацій [17].

Отже, праці вищезгаданих науковців формують цілісну картину платформного капіталізму та цифрового неофеодалізму. Для України ці концепції є критичними в умовах війни, економічної вразливості та необхідності захисту цифрового суверенітету. Розвиток національних цифрових екосистем, посилення інформаційної безпеки та підтримка відкритих технологій можуть допомогти протистояти неофеодальним тенденціям і забезпечити демократичний контроль над цифровим простором.

Формулювання мети статті. Метою статті є проаналізувати вплив цифрового неофеодалізму на політичні та соціально-економічні процеси в Україні.

Дослідження цифрового неофеодалізму в контексті України спрямоване на аналіз трансформації політичних і соціально-економічних структур під впливом глобальних технологічних платформ, які концентрують владу, ресурси

та контроль над інформаційними потоками. Методи дослідження включають концептуалізацію та SWOT-аналіз цифрового неофеодалізму.

Концептуалізація цифрового неофеодалізму спирається на критичний аналіз літератури. Н. Срнічек визначає платформи як посередників, що генерують ренту через монополізацію даних, створюючи економіку, де традиційні капіталістичні механізми поступаються рентоорієнтованим структурам [14]. М. Кастельс концептуалізує мережеву владу, яка виникає через контроль комунікаційних технологій, концентруючи політичний і соціальний вплив у корпорацій [2]. Н. Коулдрі та У. Мехіас вводять поняття «колоніалізму даних», порівнюючи експлуатацію даних із феодальним привласненням ресурсів, де користувачі стають аналогами кріпаків [3]. Е. Тагізаде та Е. Ахмадов описують глобальну боротьбу за цифрову інфраструктуру, де платформи встановлюють залежність через контроль технологій і даних [15].

Синтезуючи ці підходи, цифровий неофеодалізм доцільно визначити як систему, що характеризується трьома рисами: монополізацією даних як стратегічного ресурсу, рентоорієнтованою економікою платформ, що отримує прибуток через посередництво, і мережевою владою, яка посилює асиметрію між технічними гігантами (Meta, Google, Amazon) і національними суб'єктами. В українському контексті ця концепція набуває унікального значення через російсько-українську війну, яка робить інформаційну залежність критичною загрозою, і через амбітні цифрові ініціативи, такі як «Дія», спрямовані на зміцнення суверенітету.

SWOT-аналіз є методом стратегічного планування, який передбачає систематизацію внутрішніх і зовнішніх факторів для оцінки поточного стану та перспектив розвитку об'єкта дослідження. Внутрішні фактори включають сильні сторони, що відображають ресурси та конкурентні переваги, і слабкі сторони, що вказують на обмеження та вразливості. Зовнішні фактори охоплюють можливості, які створюють сприятливі умови для розвитку, і загрози, що становлять ризики чи перешкоди. У контексті цифрового неофеодалізму, який характеризується монополізацією даних, рентоорієнтованою економікою платформ і мережевою владою, SWOT-аналіз дозволяє оцінити здатність України протистояти викликам, пов'язаним із концентрацією цифрової влади в руках глобальних техгігантів, таких як Meta, Google чи Amazon, і водночас використовувати наявні ресурси для зміцнення цифрового суверенітету.

Сильні сторони України в умовах цифрового неофеодалізму зумовлені розвитком ІТ-сектором, який генерує 7% ВВП і забезпе-

чує 200 000 робочих місць, створюючи технологічний і кадровий потенціал для розвитку національних цифрових екосистем. Додаток «Дія», що інтегрує державні послуги, охоплює 19 мільйонів користувачів і є прикладом успішної реалізації цифрового суверенітету, зменшуючи залежність від іноземних платформ у сфері державного управління. Високий рівень суспільної довіри до «Дії» посилює її потенціал як альтернативи глобальним сервісам. Стратегічна підтримка цифровізації з боку держави, і міжнародних партнерів, таких як ЄС, створює нормативну основу для протидії монополізації цифрового простору технічними гігантами. Досвід протидії в умовах російсько-української війни, що триває з 2014 року, розвинув унікальні компетенції в інформаційній безпеці, зокрема в моніторингу та протидії дезінформації, що є конкурентною перевагою в умовах мережевої влади, описаної М. Кастельсом [2].

Слабкі сторони України проявляються в залежності від іноземних хмарних сервісів, зокрема Amazon Web Services, які використовуються для функціонування «Дії», що створює ризики втрати контролю над даними громадян і відповідає концепції «колоніалізму даних», запропонованій Н. Коулдрі та У. Мехіасом [3]. Цифровий розрив охоплює 30% населення, де доступ до інтернету обмежений швидкістю менше 10 Мбіт/с, що корелює з рівнем безробіття і поглиблює соціальну нерівність, створюючи форму «цифрового кріпацтва». Низький рівень цифрової грамотності, підвищує вразливість до дезінформації, що ускладнює протидію інформаційним маніпуляціям, які посилюються алгоритмами іноземних платформ. Обмежені фінансові ресурси, спрямовані на цифрову інфраструктуру, що складають лише 2% державного бюджету, і відсутність законодавства, подібного до європейського GDPR, знижують здатність України конкурувати з технічними гігантами, чия капіталізація, як-от Google, сягає 2 трильйонів доларів, що вдесятеро перевищує ВВП України.

Можливості для України в умовах цифрового неофеодалізму пов'язані з потенціалом розширення «Дії» як суверенної платформи, яка може охопити ширший спектр послуг і зменшити залежність від іноземних технічних гігантів, подібно до досвіду Індії з платформою Aadhaar, що знизила вплив зовнішніх сервісів на 20% за п'ять років. Інтеграція європейських стандартів захисту даних, зокрема GDPR, відкриває перспективи для регулювання діяльності Meta, Google, забезпечуючи захист персональних даних і стимулюючи конкуренцію. Інвестиції в розбудову 5G-мереж і цифрової інфраструктури за підтримки

міжнародними партнерами, такими як ЄБРР, можуть усунути цифровий розрив, що, за оцінками, здатне підвищити ВВП на 1,5% за кожні 10% зростання доступу до інтернету. Міжнародна співпраця в сфері кібербезпеки, зокрема з CERT-EU, створює можливості для посилення захисту від кібератак, подібних до WannaCry, яка завдала Україні збитків на 0,5 мільярда доларів. Розвиток відкритих технологічних екосистем, які запропоновані А. Полін [12], можуть сприяти демократизації цифрового простору, зменшуючи монополії платформ і створюючи умови для інновацій.

Загрози для України зумовлені російською агресією, яка посилює інформаційну залежність: 65% інформаційних потоків про Україну в соціальних мережах контролюються іноземними платформами, що сприяє поширенню дезінформації та ускладнює формування незалежних наративів. Кібератаки підкреслюють вразливість критичної інфраструктури через залежність від іноземного програмного забезпечення, що відповідає концепції технофеодалізму, який описаний Е. Тагізаде та Е. Ахмадовим [15]. Економічна залежність від платформної економіки, де 15% ІТ-фрілансерів втрачають до 20% доходу на комісії платформ, таких як Upwork, послаблює фінансову автономію, відображаючи рентоорієнтовану модель, запроповану Н. Срничком [14]. Глобальна монополізація цифрового простору технічними гігантами, чії ресурси значно перевищують національні бюджети, ускладнює конкуренцію для українських платформ. Геополітична нестабільність і обмежені ресурси можуть уповільнити реалізацію стратегій цифровізації, посилюючи асиметрію між Україною та глобальними платформами.

Поєднання сильних сторін і можливостей генерує нову стратегічну перспективу, а саме створення української цифрової екосистеми, яка може конкурувати з глобальними платформами, спираючись на синергію технологічних ресурсів і міжнародної підтримки. Ця екосистема може стати регіональним хабом для інновацій, використовуючи розвинений ІТ-сектор і довіру до «Дії» для залучення інвестицій у локальні стартапи, що розробляють альтернативи іноземним сервісам, як-от платіжні системи чи соціальні мережі. Впровадження GDPR за підтримки ЄС може не лише захистити дані, а й позиціонувати Україну як лідера цифровізації в Східній Європі, залучаючи партнерів із країн із подібними викликами, як-от Грузія чи Молдова. Співпраця з НАТО в кібербезпеці може трансформувати національні компетенції в експортний продукт, наприклад, через створення консалтингових

центрів із протидії дезінформації, що генеруватиме економічні та політичні дивіденди. Інвестиції в 5G можуть стимулювати розвиток децентралізованих мереж, які зменшать залежність від централізованих платформ, подібно до ініціатив із блокчейн-технологій в Естонії.

Поєднання сильних сторін і загроз формує новий виклик, тобто необхідність створення гібридної моделі цифрового захисту, яка поєднує технологічні інновації з дипломатичними зусиллями для протидії інформаційним і кіберзагрозам. Алгоритми іноземних платформ, що посилюють дезінформацію в умовах російської агресії, вимагають розробки національних систем модерації контенту, які використовуватимуть штучний інтелект, створений ІТ-сектором, для протидії маніпуляціям, зберігаючи свободу слова. Кібератаки актуалізують потребу в локалізованих центрах обробки даних, які, спираючись на «Дію», можуть забезпечити безпеку критичної інфраструктури навіть у разі глобальних збоїв. Економічна залежність від платформ, таких як Upwork, вимагає створення національних фріланс-платформ, які інтегруються з «Дією» для зниження комісій і підтримки українських талантів. Монополізація технічних гігантів і геополітична нестабільність змушують Україну шукати асиметричні стратегії, як-от партнерства з нейтральними країнами чи міжнародними організаціями, щоб компенсувати брак ресурсів і забезпечити стійкість цифрових ініціатив.

Поєднання слабких сторін і можливостей відкриває нову перспективу, а саме трансформацію обмежень у драйвери інклюзивного розвитку через цілеспрямовані реформи та міжнародну співпрацю. Залежність від іноземних хмарних сервісів може бути перетворена на можливість створення гібридних моделей даних, де локальні сервери, підтримані GDPR, обробляють критичні дані, а іноземні сервіси використовуються для некритичних функцій, знижуючи ризики «колоніалізму даних». Цифровий розрив і низька цифрова грамотність можуть стати основою для національної програми цифрової освіти, інтегрованої в «Дію», яка використовуватиме 5G для доставки навчального контенту в регіони, подібно до освітніх платформ в Індії. Обмежені інвестиції в інфраструктуру можуть бути компенсовані через співпрацю з НАТО, що забезпечить не лише технічну, а й фінансову підтримку для створення кіберзахисних хабів. Відсутність законодавства, подібного до GDPR, може стимулювати розробку унікального національного стандарту захисту даних, який враховує контекст гібридної війни та залучає експертизу відкритих екосистем для забезпечення прозорості.

Поєднання слабких сторін і загроз створює новий критичний виклик, тобто ризик цифрової ізоляції, якщо обмеження не будуть подолані в умовах зростаючого тиску від зовнішніх загроз. Залежність від іноземних сервісів у поєднанні з кібератаками може призвести до втрати довіри до цифрових систем, таких як «Дія», якщо дані громадян будуть пошкоджені, або оприлюднені, що вимагатиме створення резервних офлайн-систем для критичних державних функцій. Цифровий розрив і низька цифрова грамотність у контексті дезінформації, в контексті російської агресії, можуть сприяти соціальній поляризації українського соціуму. Обмежені інвестиції в поєднанні з монополізацією технічних гігантів можуть зафіксувати роль України в якості периферійного постачальника робочої сили для платформ, якщо не будуть створені локальні альтернативи. Відсутність законодавства в умовах геополітичної нестабільності може призвести до втрати контролю над інформаційними потоками, що вимагатиме створення міжнародних коаліцій для тиску на технічних гігантів з метою дотримання національних інтересів.

Аналіз поєднань SWOT-елементів генерує нові стратегічні інсайти з варіативності від створення національної цифрової екосистеми та гібридної моделі захисту до трансформації обмежень у драйвери розвитку та протидії ризику цифрової ізоляції. Ці перспективи підкреслюють необхідність комплексної стратегії, яка включає локалізацію даних, інвестиції в освіту та інфраструктуру, розвиток національних стандартів і міжнародну співпрацю. Це дасть змогу Україні не лише протистояти цифровому неофеодализму, а й стати регіональним лідером у цифровій трансформації.

SWOT-аналіз демонструє, що Україна володіє значним потенціалом для протидії цифровому неофеодализму завдяки розвиненому ІТ-сектору, успішному впровадженню «Дії» та міжнародній підтримці. Україна при цьому стикається з критичними обмеженнями через цифровий розрив, низьку цифрову грамотність і залежність від іноземних сервісів. Можливості розширення суверенних платформ, інтеграції європейських стандартів і подолання цифрового розриву можуть бути реалізовані лише за умови ефективного протистояння загрозам російської агресії, кібератак і економічної залежності. Стратегічний акцент на локалізацію даних, інвестиції в цифрову інфраструктуру та освіту, а також впровадження регуляторних механізмів для обмеження впливу технічних гігантів є критично важливим для забезпечення цифрового суверенітету та інклюзивного розвитку України в умовах цифрового неофеодализму.

Висновки. Цифровий неофеодализм, що характеризується монополізацією даних, рентоорієнтованою економікою платформ і мережевою владою, становить для України як серйозні виклики, так і можливості для зміцнення цифрового суверенітету, економічної автономії та соціальної інклюзивності.

SWOT-аналіз систематизує сильні та слабкі сторони, можливості та загрози, генеруючи нові стратегічні інсайти через їхні поєднання. Сильні сторони України, зокрема розвинений ІТ-сектор, успішне впровадження «Дії» та міжнародна підтримка, створюють основу для розвитку національної цифрової екосистеми, яка може стати регіональним хабом для інновацій і протистояти монополізації технічних гігантів. Поєднання цих сильних сторін із можливостями, такими як інтеграція GDPR, інвестиції в 5G і співпраця з НАТО, відкриває перспективу позиціонування України як лідера цифровізації, заснованої на принципах етики, в Східній Європі, здатного залучати партнерів із країн із подібними викликами, як-от Грузія чи Молдова. Ця екосистема може підтримувати локальні стартапи, які спрямовані на розробку альтернатив іноземним сервісам, як-от платіжні системи чи соціальні мережі, а співпраця в кібербезпеці може трансформувати національні компетенції в експортний продукт, наприклад, консалтингові центри з протидії дезінформації.

Поєднання сильних сторін із загрозами, такими як російська агресія, кібератаки та економічна залежність від платформ, формує виклик створення гібридної моделі цифрового захисту, яка поєднує технологічні інновації з дипломатичними зусиллями. Національні системи модерації контенту на основі штучного інтелекту, локалізовані центри обробки даних, інтегровані з «Дією», та національні фріланс-платформи можуть зменшити вразливість до дезінформації, кібератак і економічної експлуатації. Асиметричні стратегії, як-от партнерства з нейтральними країнами чи міжнародними організаціями, допоможуть компенсувати брак ресурсів у контексті геополітичної нестабільності та монополізації технічних гігантів.

Слабкі сторони, зокрема залежність від іноземних хмарних сервісів, цифровий розрив, низька цифрова грамотність і відсутність законодавства, подібного до GDPR, у поєднанні з можливостями створюють перспективу трансформації обмежень у драйвери інклюзивного розвитку. Гібридні моделі даних, де локальні сервери обробляють критичні дані, національні програми цифрової освіти через «Дію» з використанням 5G і розробка унікального

стандарту захисту даних можуть компенсувати слабкості та позиціонувати Україну як інноваційну державу. Співпраця з ЄБРР і НАТО забезпечить ресурси для створення кіберзахисних хабів і подолання цифрового розриву.

Поєднання слабких сторін із загрозами підкреслює ризик цифрової ізоляції, якщо обмеження не будуть подолані. Втрата довіри до цифрових систем через кібератаки, соціальна поляризація українського соціуму через цифровий розрив і периферійна роль у платформній економіці можуть посилити залежність від технічних гігантів. Для протидії цьому необхідні резервні офлайн-системи для критичних функцій, кампанії з медіаграмотності та міжнародні коаліції для тиску на платформи з метою дотримання національних інтересів.

На основі SWOT-аналізу пропонуються стратегічні рекомендації, а саме локалізація даних і розвиток національних платформ, інте-

грованих із «Дією», для зменшення залежності від технічних гігантів; інвестиції в 5G-мережі та цифрову освіту для усунення цифрового розриву; розробка національного стандарту захисту даних і інтеграція GDPR для обмеження впливу платформ; посилення співпраці з ЄС, НАТО та нейтральними країнами для залучення ресурсів; розвиток відкритих технологічних екосистем для демократизації цифрового простору. Ці заходи сприятимуть формуванню стійкої, суверенної та конкурентоспроможної цифрової політики, яка дозволить Україні протистояти викликам цифрового неофеодалізму та зміцнити свою позицію на регіональній і глобальній арені. Перспективні напрямки досліджень можуть бути пов'язані із дослідженням національних цифрових екосистем як інструменту забезпечення цифрового суверенітету та етикою та регулюванням цифрових технологій.

Література:

1. Bremmer I. *Us vs. Them: The Failure of Globalism*. Portfolio, 2018. 208 p.
2. Castells M. *Communication Power*. Oxford University Press, 2011. 592 p.
3. Couldry N. & Mejias U. A. *The Costs of Connection*. Stanford University Press, 2019. 352 p.
4. Dean J. 'Communism or Neo-Feudalism? *New Political Science*. 2020. № 42(1). P. 1–17.
5. Durand C. Techno-feudalism: The Making of the Digital Economy. Verso, 2024. 240 p.
6. Gal Yoav & Gal Adiv Knowledge Bias: Neo-feudalism and Other Reasons to Avoid Sharing Knowledge by Knowledge Workers, Springer. Portland International Center for Management of Engineering and Technology (PICMET). *Journal of the Knowledge Economy*. 2019. Vol. 10(2), P. 826–848
7. Gstrein O. J., & Kochenov D. Digital Identity and Distributed Ledger Technology: Paving the Way to a Neo-Feudal Brave New World? *Frontiers in Blockchain*. 2020. № 3, Article 10.
8. Jensen J. L. The return of medieval society –control, surveillance and neo-feudalism in the age of the internet The 20th Annual Conference of the Association of Internet Researchers Brisbane, Australia, 2019. 2–5 October P. 1–4
9. Kotkin J. *The Coming of Neo-Feudalism* Encounter Books, USA. 2023. 296 p.
10. Luis S. Entering the neo-feudal ? Art and resistance in the age of platform capitalism. 2024. March 2nd. URL: https://www.academia.edu/123039936/ENTERING_THE_NEO_FEUDAL_ART_AND_RESISTANCE_IN_THE_AGE_OF_PLATFORM_CAPITALISM (accessed: 24.05.2025)
11. Patelis K. Have I Got News for You: The Road to Neo-feudalism. *Media Theory*. 2024. № 8(2). P. 127–146
12. Paulin A. Technological Ecosystems' Role in Preventing Neo-Feudalism in Smart-City Informatization. WWW 16 Companion: Proceedings of the 25th International Conference Companion on World Wide Web. P. 333–337
13. Reitz T. Academic hierarchies in neo-feudal capitalism: how status competition processes trust and facilitates the appropriation of knowledge. 2017. Volume 73. P. 871–886
14. Srnicek N. *Platform Capitalism*. Polity Press. 2016. 120 p
15. Taghizade E., Ahmadov E. Techno Feudalism and the New Global Power Struggle: Echoes of a Digital Cold War. *International journal of research and innovation in social science (Ijriiss)*. 2025. Volume IX Issue II February P. 1144–1170
16. Wollenberg D. Chapter 4 – Anxious Returns: The New Feudalism and New Medievalis. *Medieval Imagery in Today's Politics* Amsterdam University Press, 2018. P. 65–86
17. Yan J. Techno-Feudalism as Primitive Accumulation: A Marxist Perspective on Digital Capitalism. *Critical Sociology*. 2024. № 2. URL: <https://journals.sagepub.com/doi/abs/10.1177/08969205241302838> (accessed: 24.05.2025)
18. Zafirovsk M. Neo-Feudalism' in America? Conservatism in Relation to European Feudalism. *International Review of Sociology*. 2007. № 17(3). P. 393–427

Дата надходження статті: 25.05.2025

Дата прийняття статті: 03.06.2025

Опубліковано: 01.10.2025