Розділ 5
ЗОВНІШНЯ ПОЛІТИКА ТА НАЦІОНАЛЬНА БЕЗПЕКА

http://doi.org/10.26565/1727-6667-2025-2-19
УДК 351.86:004(477)

Дзюндзюк Вячеслав Борисович,
доктор наук з державного управління, професор,
завідувач кафедри публічної політики
Навчально-наукового інституту «Інститут державного управління»
Харківського національного університету імені В.Н. Каразіна
майдан Свободи, 4, м. Харків, 61022, Україна
ORCID ID: http://orcid.org/0000-0003-0622-2600
e-mail: vbdzun@gmail.com

ФОРМУВАННЯ ЦИФРОВОЇ ЕКОСИСТЕМИ НАЦІОНАЛЬНОЇ БЕЗПЕКИ ДЛЯ ПРОТИДІЇ ГІБРИДНИМ ЗАГРОЗАМ

Анотація. Гібридні загрози, що поєднують військові, інформаційні, кібернетичні, економічні та дипломатичні інструменти впливу, становлять одну з найсерйозніших проблем для національної безпеки у XXI столітті. Традиційні моделі організації систем безпеки, побудовані на принципах департаменталізації та вертикальної ієрархії, виявляють обмежену ефективність у протидії загрозам, які за своєю природою є багатовимірними, динамічними та транскордонними. Досвід України, яка з 2014 року протистоїть масштабній гібридній агресії, демонструє критичну необхідність інтеграції різнорідних безпекових акторів, технологій та процесів у єдину цифрову екосистему, здатну забезпечити синергетичний ефект у виявленні, аналізі та нейтралізації загроз. Метою статті є розробка концептуальної моделі цифрової екосистеми національної безпеки та визначення ключових принципів, архітектурних рішень та інституційних механізмів її формування в умовах гібридної війни.

У статті обґрунтовується, що ефективна цифрова екосистема національної безпеки має базуватися на п'яти взаємопов'язаних компонентах: інформаційно-аналітична інфраструктура для збору та обробки даних з різнорідних джерел; технологічна платформа, що інтегрує штучний інтелект, великі дані, блокчейн та засоби кібербезпеки; аналітичні інструменти для трансформації даних у дієву інформацію; процесні механізми координації та прийняття рішень; система управління, що визначає правила взаємодії між державними, приватними та громадянськими акторами. Кожен компонент виконує специфічні функції, але їх ефективність досягається лише через тісну інтеграцію та взаємодію.

Аналіз міжнародного досвіду показує, що найбільш ефективні екосистеми характеризуються балансом централізованої координації та децентралізованої ініціативи, поєднанням державного регулювання та ринкової конкуренції, інтеграцією технологічних можливостей та інституційних механізмів довіри. Ізраїльська модель демонструє переваги тісної інтеграції між оборонним сектором, академією та приватним бізнесом. Естонська модель показує ефективність розподіленої архітектури та міжнародного партнерства. Американський досвід підкреслює важливість спеціалізованих координаційних агенцій. Сінгапурська практика ілюструє можливості централізованого планування при збереженні ролі приватного сектору.

Український контекст висуває специфічні вимоги до формування екосистеми: необхідність функціонування в умовах активного конфлікту, обмеженість ресурсів порівняно з державою-агресором, наявність застарілих систем та інституційних бар'єрів, високий рівень корупційних ризиків. Водночас Україна володіє значними можливостями: потужний інноваційний потенціал ІТ-сектору, досвід протидії гібридним загрозам, накопичений за десятиліття конфлікту, міжнародна підтримка від партнерів, високий рівень мобілізації громадянського суспільства та готовність до співпраці з державними структурами безпеки. Сформульовано рекомендації щодо поетапного впровадження екосистемного підходу з пріоритизацією критичних функцій, використанням швидких перемог для створення інституційного імпульсу, забезпеченням багатошарової кібербезпеки та розвитком компетенцій персоналу на всіх етапах трансформації.

Ключові слова: *публічне управління, цифрова екосистема, національна безпека, гібридні загрози, міжвідомча координація, штучний інтелект, кібербезпека, цифрова трансформація, державно-приватне партнерство.*

Як цитувати: Дзюндзюк В. Б. Формування цифрової екосистеми національної безпеки для протидії гібридним загрозам *Теорія та практика державного управління.* 2025. Вип. 2 (81). С. 315–330. http://doi.org/10.26565/1727-6667-2025-2-19

Вступ. Характер загроз національній безпеці зазнав радикальної трансформації у першій чверті XXI століття. Якщо у період Холодної війни домінуючими були загрози військового характеру з чітко ідентифікованими джерелами та інструментами протидії, то сучасний безпековий ландшафт визначається гібридними загрозами – складними, багатовимірними феноменами, що поєднують військові операції, кібератаки, дезінформаційні кампанії, економічний тиск, дипломатичну ізоляцію та маніпулювання внутрішньополітичними процесами [14]. Гібридна війна РФ проти України, розпочата у 2014 році анексією Криму та підтримкою сепаратистів на Донбасі, ескальована до повномасштабного вторгнення у лютому 2022 року, стала найбільш комплексним прикладом застосування гібридних стратегій у сучасній історії. Цей конфлікт продемонстрував як критичні вразливості традиційних систем безпеки, побудованих на принципах відомчої автономії та вертикальної ієрархії, так і можливості їх трансформації через систематичне впровадження цифрових технологій та екосистемних принципів організації.

Цифрові технології радикально змінюють як природу загроз, так і можливості протидії їм. З одного боку, цифровізація створює принципово нові вектори атак: критична інфраструктура стає вразливою до кібератак, які можуть паралізувати енергопостачання, транспорт, фінансові системи. Соціальні медіа перетворюються на платформи для масових дезінформаційних кампаній, здатних впливати на громадську думку, підривати довіру до інститутів, провокувати соціальну поляризацію. Штучний інтелект використовується для створення дипфейків – синтетичних відео та аудіо, що імітують реальних людей, для автоматизації пропагандистських операцій через боти та тролінгові мережі [7]. З іншого боку, ті самі технології надають безпрецедентні можливості для раннього виявлення загроз через аналіз величезних масивів даних, координації відповідей між різними відомствами в режимі реального часу, підтримки прийняття рішень в умовах невизначеності через предиктивну аналітику та системи моделювання [5].

Традиційна організація систем національної безпеки, побудована на принципах департаменталізації та вертикальної ієрархії, де різні відомства – міністерство оборони, служби безпеки, правоохоронні органи, кіберполіція, прикордонна служба – функціонують у значній мірі автономно зі слабкою координацією та обмеженим обміном інформацією, виявляється структурно неспроможною ефективно протидіяти гібридним загрозам. Гібридні атаки за своєю природою є транссекторальними: одна й та сама кампанія може одночасно включати кібератаки на критичну інфраструктуру, дезінформацію в соціальних медіа, економічний тиск через енергетичні важелі, дипломатичну ізоляцію та загрозу військової ескалації. Жоден окремий орган не володіє всією необхідною інформацією, аналітичними спроможностями та інструментами для адекватної відповіді на такі комплексні виклики. Відомча фрагментація призводить до дублювання зусиль, неузгоджених дій, повільного реагування та неефективного використання обмежених ресурсів [19].

Концепція екосистеми, що виникла спочатку в біологічних науках для опису взаємозалежних спільнот організмів та їх середовища, а згодом була адаптована для аналізу бізнес-організацій, інновацій та цифрових платформ, пропонує альтернативну парадигму організації систем національної безпеки [11]. Екосистема передбачає не ієрархічне підпорядкування всіх елементів єдиному центру, а взаємозалежну мережу різноманітних акторів – державних агенцій, приватних компаній, дослідницьких центрів, громадських організацій, міжнародних партнерів – які обмінюються ресурсами, інформацією, аналітичними можливостями для досягнення спільних цілей при збереженні організаційної автономії у вирішенні специфічних завдань. Цифрова екосистема національної безпеки інтегрує цих різнорідних учасників через загальні цифрові платформи, стандартизовані протоколи обміну даними, спільні аналітичні інструменти та узгоджені механізми координації.

Формування цифрової екосистеми національної безпеки є особливо актуальним для України як держави, що протистоїть найбільш інтенсивній та багатовимірній гібридній агресії в сучасній історії. Український досвід протягом десятиліття конфлікту демонструє як фундаментальні виклики – функціонування застарілих систем, обмеженість ресурсів, бюрократичні бар'єри, корупційні ризики

– так і унікальні можливості: високий рівень цифровізації суспільства, інноваційний потенціал одного з найбільших IT-секторів Європи, мобілізація громадянського суспільства, міжнародна підтримка від партнерів. Успішні українські ініціативи, такі як платформа електронних послуг «Дія», національна система реагування на кіберінциденти CERT-UA, волонтерська IT Army, проекти верифікації інформації, ілюструють потенціал екосистемного підходу для створення ефективних рішень в умовах обмежених ресурсів та активного конфлікту.

Огляд літератури. Проблематика формування цифрових екосистем у сфері національної безпеки є відносно новою міждисциплінарною областю, що перебуває на перетині теорії організаційних екосистем, студій цифрової трансформації, досліджень гібридних конфліктів, кібербезпеки та публічного управління в умовах кризи. Концептуальні основи екосистемного підходу до організації складних систем були закладені у працях Moore [16], який запровадив поняття бізнес-екосистеми як мережі взаємозалежних організацій, що спільно створюють та привласнюють цінність, еволюціонують разом навколо спільних інновацій. Jacobides, Cennamo та Gawer [11] розширили це розуміння, виділяючи структурні елементи екосистем: багатосторонні платформи як технологічну основу взаємодії, механізми управління взаємозалежністю між різнорідними учасниками, правила розподілу створеної цінності, бар'єри входу та виходу. Adner [1] наголошує на критичній ролі вирівнювання очікувань та координації діяльності між учасниками екосистеми для досягнення колективних результатів, що перевищують можливості окремих організацій.

Застосування екосистемного підходу до сфери безпеки та управління ризиками аналізується у працях Vespignani [20], який досліджує мережеві ефекти у поширенні загроз та координації відповідей, демонструючи, що ефективність протидії епідеміям, кібератакам чи дезінформації залежить не лише від спроможностей окремих акторів, а критично від топології, щільності та якості зв'язків між ними. Jackson [10] розглядає питання створення екосистем кібербезпеки, що об'єднують урядові агенції, приватні компанії, які володіють більшістю критичної інфраструктури, та дослідницькі центри для обміну інформацією про загрози, спільної розробки захисних рішень, координації реагування на інциденти. Bryson, Crosby та Stone [4] аналізують виклики міжсекторальної співпраці у сфері публічної безпеки, виділяючи бар'єри довіри, несумісність організаційних культур, конфлікти інтересів та пропонуючи механізми їх подолання.

Цифрова трансформація систем національної безпеки досліджується у працях Coaffee та Lee [6], які аналізують вплив технологій великих даних, штучного інтелекту та Інтернету речей на можливості виявлення та попередження загроз, переосмислення концепції стійкості міських систем. Dunn [7] досліджує еволюцію кібербезпеки від технічної проблеми до стратегічного виміру національної безпеки, аналізуючи трансформацію інститутів, політик та міжнародної співпраці. Buchanan [5] розглядає геополітичні наслідки розвитку штучного інтелекту для балансу сил, характеру конфліктів, стримування та стабільності, виділяючи AI triad – взаємозв'язок між даними, обчислювальними потужностями та алгоритмами як основу технологічного лідерства.

Гібридна війна як феномен сучасних конфліктів концептуалізована у працях Hoffman [9], який визначає гібридні загрози як конвергенцію фізичних та психологічних, кінетичних та некінетичних, військових та невійськових, державних та недержавних засобів для досягнення політичних цілей. Berzins [3] аналізує роль інформаційних операцій у російських гібридних кампаніях проти України та Сирії, виявляючи патерни координації між різними інструментами впливу. Lanoszka [14] досліджує виклики, які гібридна війна створює для традиційних концепцій стримування та колективної оборони в контексті НАТО.

Цифрове врядування та трансформація публічного управління досліджуються Margetts та Dunleavy [15], які виділяють діджиталізацію, реінтеграцію фрагментованих процесів, потребо-орієнтовану холістичність як ключові тренди другої хвилі цифрового врядування. Janowski [12] пропонує багатовимірну модель цифрового врядування, що охоплює технологічний, інституційний, соціальний виміри та їх взаємодію. Gil-Garcia, Dawes та Pardo [8] аналізують виклики міжорганізаційної інтеграції даних у публічному секторі, виявляючи технічні, семантичні, правові, організаційні бар'єри та шляхи їх подолання. Klievink, Bharosa та Tan [13] досліджують механізми реалізації публічних цінностей через державно-приватні інформаційні платформи.

Український досвід протидії гібридним загрозам та цифровізації безпекового сектору аналізується у працях Shelest [18], яка досліджує еволюцію української системи національної безпеки під впливом тривалого конфлікту, виявляючи інституційні адаптації, зміни доктрин, розвиток нових спроможностей. Wilson [21] аналізує роль волонтерського руху та громадянського суспільства у доповненні державних структур безпеки, створенні неформальних мереж співпраці.

Аналіз літератури виявляє прогалину у дослідженнях, які б інтегрували екосистемний підхід, цифрові технології та специфіку протидії гібридним загрозам у єдину концептуальну модель, призначену спеціально для трансформації публічного управління національною безпекою. Більшість праць зосереджена на окремих аспектах – або на екосистемах у бізнес-контексті, або на технологіях без інституційного виміру, або на гібридних загрозах без систематичного аналізу цифрових рішень – без комплексного бачення архітектури, принципів, механізмів формування та функціонування цифрової екосистеми безпеки.

Мета статті. Метою статті є розробка концептуальної моделі цифрової екосистеми національної безпеки для протидії гібридним загрозам та визначення ключових принципів, архітектурних рішень, інституційних механізмів та етапів її формування в умовах обмежених ресурсів, інституційних обмежень та активного конфлікту з урахуванням специфіки публічного управління.

Методологія дослідження. Дослідження базується на міждисциплінарному підході, що інтегрує теорію організаційних екосистем з концепціями цифрової трансформації та студіями гібридних конфліктів. Системний аналіз використано для виявлення взаємозв'язків між компонентами цифрової екосистеми національної безпеки, ідентифікації критичних залежностей та точок інтеграції. Компаративний метод застосовано для аналізу міжнародного досвіду формування безпекових екосистем у США, Ізраїлі, Естонії, Сінгапурі, виявлення кращих

практик та їх адаптивності до українського контексту. Метод теоретичного моделювання дозволив розробити концептуальну п'ятишарову архітектуру цифрової екосистеми з визначенням функцій кожного компонента та механізмів їх взаємодії. Кейс-метод використано для дослідження українського досвіду, включаючи аналіз ініціатив «Дія» як платформи цифрових послуг, системи кібербезпеки CERT-UA, проектів державно-приватного партнерства у сфері оборонних технологій, волонтерських ініціатив IT Army та верифікації інформації.

Основні результати дослідження. Цифрова екосистема національної безпеки являє собою взаємопов'язану мережу державних органів, приватних компаній, наукових установ, громадянського суспільства та міжнародних партнерів, які через загальні цифрові платформи, стандартизовані протоколи обміну даними, спільні аналітичні інструменти та узгоджені механізми координації спільно створюють інтегровані спроможності виявлення, аналізу, попередження та нейтралізації гібридних загроз у режимі, наближеному до реального часу. На відміну від традиційної ієрархічної моделі, де кожен актор функціонує переважно автономно в межах своєї юрисдикції з обмеженою взаємодією, екосистемний підхід передбачає горизонтальну інтеграцію через цифрові технології, створення мережевої архітектури зв'язків, розподілену аналітику при збереженні організаційної автономії учасників у вирішенні специфічних завдань та прийнятті рішень у своїх сферах компетенції.

Концептуальна архітектурна модель цифрової екосистеми національної безпеки включає п'ять взаємопов'язаних функціональних шарів, кожен з яких виконує специфічні функції, але тісно інтегрований з іншими. Перший, базовий шар – інформаційно-аналітична інфраструктура, що забезпечує безперервний збір, надійне зберігання та первинну обробку даних з максимально широкого спектру різнорідних джерел. Це включає розгалужену мережу сенсорів Інтернету речей, розміщених на об'єктах критичної інфраструктури для моніторингу фізичних параметрів та виявлення аномалій, системи автоматизованого моніторингу соціальних медіа та інформаційного простору для раннього виявлення дезінформаційних кампаній та маніпуляцій, канали надходження класифікованої розвідувальної інформації від спеціалізованих служб, масиви даних з відкритих джерел включно з новинами, академічними публікаціями, урядовими звітами, системи захисту периметру та моніторингу кіберзагроз, економічні та фінансові індикатори, дані про рух через кордони, супутникові знімки та геопросторову інформацію [13]. Критичним викликом на цьому рівні є забезпечення технічної інтероперабельності між різними системами через впровадження стандартизованих протоколів обміну даними, створення єдиних онтологій та семантичних моделей, розробку API для інтеграції, дотримання принципів захисту персональних даних та конфіденційності.

Другий шар – технологічна платформа, що інтегрує передові цифрові технології для трансформації сирих даних у аналітичну інформацію та підтримки прийняття рішень. Системи штучного інтелекту та машинного навчання використовуються для автоматичного виявлення аномалій у поведінці систем, розпізнавання складних патернів гібридних атак, що розгортаються одночас-

но у кількох доменах, класифікації загроз за рівнем критичності, предиктивної аналітики для прогнозування ймовірних векторів майбутніх атак на основі історичних даних та поточних індикаторів [5]. Технології обробки природної мови застосовуються для аналізу величезних обсягів текстової інформації в соціальних медіа, новинних джерелах, форумах з метою виявлення координованих дезінформаційних кампаній, ідентифікації ботів та тролінгових мереж, аналізу сентименту та динаміки громадської думки. Системи комп'ютерного зору використовуються для виявлення діпфейків – синтетичних відео та зображень, створених за допомогою генеративних нейромереж, аналізу супутникових знімків для моніторингу військових переміщень, верифікації автентичності візуального контенту. Технології блокчейн та розподілених реєстрів забезпечують незмінність критичних записів, захист ланцюгів постачання від маніпуляцій, створення систем цифрової ідентифікації, що стійкі до підробки [2]. Квантові технології розглядаються як перспективний напрям для створення принципово захищених каналів комунікації, стійких до перехоплення, хоча їх практичне впровадження ще обмежене технологічною зрілістю [7].

Третій шар – аналітичні інструменти та системи підтримки прийняття рішень, що трансформують технологічні можливості у практичні рішення для осіб, які приймають рішення на різних рівнях. Платформи візуалізації даних представляють складну багатовимірну інформацію у інтуїтивно зрозумілій графічній формі – карти загроз у реальному часі, дашборди з ключовими індикаторами, мережеві графи взаємозв'язків між акторами, часові лінії розгортання кампаній. Системи моделювання та симуляції дозволяють прогнозувати розвиток ситуацій при різних сценаріях, оцінювати потенційні наслідки альтернативних варіантів відповіді, проводити віртуальні навчання та тестування процедур реагування без ризиків для реальних систем. Платформи для спільної роботи та аналізу забезпечують можливість командам аналітиків з різних відомств одночасно працювати над спільними завданнями, обмінюватися гіпотезами та оцінками, інтегрувати різні перспективи для створення більш повної картини [4]. Експертні системи акумулюють знання досвідчених фахівців у формалізованих базах знань, надають рекомендації менш досвідченим аналітикам, забезпечують консистентність оцінок.

Четвертий шар – процесні механізми та протоколи, що визначають правила та процедури взаємодії, координації та спільних дій між різними учасниками екосистеми. Це включає чітко формалізовані протоколи обміну інформацією, які специфікують який тип інформації, в якому форматі, через які канали, з якими рівнями класифікації передається між різними агенціями. Механізми верифікації та перехресної перевірки даних для підтвердження достовірності критичної інформації перед прийняттям рішень, особливо важливі в умовах інформаційної війни, де дезінформація може бути спеціально впроваджена для провокування неадекватних реакцій. Процедури спільного аналізу загроз, коли представники різних відомств регулярно зустрічаються для обговорення поточної ситуації, обміну оцінками, виявлення прогалин у розумінні. Алгоритми пріоритизації та розподілу завдань для ефективного використання об-

межених ресурсів – аналітичних, технічних, людських – фокусуючи їх на найбільш критичних загрозах. Системи управління інцидентами, що координують реагування на конкретні події від моменту виявлення через аналіз, прийняття рішення, виконання відповідних дій до пост-інцидентного аналізу та інтеграції уроків [10]. Критично важливим є балансування між швидкістю реагування, необхідною в умовах динамічних загроз, та належною перевіркою інформації для уникнення помилкових спрацювань, які можуть мати серйозні наслідки.

П'ятий, найвищий шар – управління екосистемою, що охоплює інституційні механізми координації, правила взаємодії, розподіл відповідальності між учасниками. Це включає створення постійно діючих міжвідомчих координаційних центрів, які виконують функції хабів екосистеми, забезпечуючи щоденну оперативну координацію між різними агенціями, без підміни їх власних функцій та повноважень. Визначення та законодавче закріплення правил доступу до даних та їх використання, що балансують потреби безпеки з правами громадян на приватність, встановлюють межі дозволеного використання персональної інформації, процедури отримання санкцій для доступу до чутливих даних. Механізми вирішення конфліктів та суперечок між учасниками екосистеми, неминучих в умовах різних організаційних культур, пріоритетів, інтересів. Стандарти кібербезпеки, обов'язкові для всіх учасників екосистеми для забезпечення мінімального рівня захисту та запобігання ситуаціям, коли найслабша ланка компрометує всю систему. Етичні принципи та керівництва щодо використання технологій штучного інтелекту, особливо в контексті автоматизованого прийняття рішень, що впливають на права людини, для запобігання зловживанням та дискримінації [15].

При цьому ключові принципи функціонування ефективної екосистеми включають відкритість при збереженні безпеки – стандартизовані відкриті інтерфейси та протоколи дозволяють новим учасникам приєднуватися до екосистеми без необхідності окремих двосторонніх інтеграцій з кожним існуючим учасником, що забезпечує масштабованість, водночас багаторівневі механізми контролю доступу, шифрування, сегментація мережі забезпечують захист критичної інформації та запобігають несанкціонованому доступу. Модульність архітектури дозволяє замінювати або оновлювати окремі технологічні компоненти без необхідності перебудови всієї системи, що критично важливо в умовах швидкої еволюції технологій та загроз. Горизонтальна масштабованість забезпечує здатність обробляти зростаючі обсяги даних та кількість учасників через додавання додаткових обчислювальних ресурсів без фундаментальної зміни архітектури. А відмовостійкість досягається через резервування критичних компонентів, географічно розподілену архітектуру, автоматичне переключення на резервні системи при відмовах, регулярне тестування процедур відновлення [10].

Формування такої екосистеми вимагає вирішення складного комплексу технічних, інституційних, правових та культурних викликів. Технічні виклики включають забезпечення реальної інтероперабельності між різнорідними системами, створеними різними виробниками в різний час з різними стандартами, що вимагає значних інвестицій у middleware, адаптери, трансляцію форматів.

Кібербезпека самих платформ екосистеми є парадоксальним викликом – система, створена для захисту від загроз, сама стає привабливою ціллю для атак, концентрація критичних даних створює єдині точки відмови, взаємозв'язок компонентів означає, що компрометація одного елемента може каскадом поширитися на всю систему. Обробка величезних обсягів даних у реальному часі вимагає потужної обчислювальної інфраструктури, ефективних алгоритмів, оптимізації використання ресурсів.

Інституційні виклики є часто більш складними за технічні. Необхідна комплексна нормативно-правова база, яка регулює обмін даними між відомствами при дотриманні принципів захисту персональної інформації та прав людини, встановлює відповідальність за неправомірне використання даних, визначає процедури доступу до різних категорій інформації. Український законодавчий ландшафт у цій сфері характеризується фрагментацією, прогалинами, застарілими нормами, що не враховують специфіку цифрових технологій та гібридних загроз. Подолання відомчих бар'єрів та культури «інформаційних силосів» є критичним викликом – агенції історично неохоче діляться інформацією через побоювання втрати організаційної автономії, контролю, бюджетів, впливу, ризиків витоку інформації до конкурентів чи опонентів, складність оцінки співвідношення ризиків та вигод від обміну. Це вимагає не лише технічних рішень, а фундаментальної зміни організаційної культури, створення системи стимулів для співпраці, демонстрації конкретних переваг від участі в екосистемі [8].

Державно-приватне партнерство є абсолютно критичним елементом екосистеми національної безпеки, оскільки значна частина критичної інфраструктури – енергетика, телекомунікації, фінанси, транспорт – належить або управляється приватним сектором, який також володіє більшістю передових технологічних спроможностей у сферах кібербезпеки, штучного інтелекту, аналізу даних. Моделі партнерства варіюються від традиційних контрактних відносин, де держава закуповує послуги чи продукти у приватних компаній, до більш складних форм спільних підприємств для розробки критичних технологій, венчурних інвестицій держави у перспективні стартапи, створення sandboxes для тестування інноваційних рішень у контрольованому середовищі, програм підтримки НДДКР у пріоритетних напрямах [13]. Український IT-сектор, який є одним з найбільших в Європі, продемонстрував високу готовність до співпраці у сфері національної безпеки, що проявилося у волонтерському створенні IT Army для проведення кібероперацій проти агресора, розробці спеціалізованого програмного забезпечення для потреб армії безкоштовно або за символічну плату, участі компаній у захисті критичної інфраструктури, створенні систем верифікації інформації. Однак інституалізація цієї співпраці, перехід від волонтерських ad-hoc ініціатив до стійких механізмів партнерства вимагає вирішення питань інтелектуальної власності, конфіденційності комерційної інформації, страхування ризиків, довгострокових зобов'язань.

Розвиток компетенцій персоналу є фундаментальним фактором успіху екосистеми, оскільки найбільш передові технології неефективні без людей, здатних їх належним чином використовувати, інтерпретувати результати, при-

ймати рішення на основі аналітики. Безпекові структури гостро потребують фахівців з аналізу даних, машинного навчання, кібербезпеки, що володіють як технічними навичками, так і розумінням специфіки предметної області. Конкуренція за таланти з приватним сектором, який пропонує значно вищі зарплати, є серйозним викликом для державних агенцій. Необхідні програми перепідготовки традиційних аналітиків розвідки, безпеки для ефективної роботи з цифровими інструментами, розуміння можливостей та обмежень технологій, критичного мислення щодо результатів автоматизованого аналізу [12]. Важлива культурна трансформація організацій від традиційної бюрократичної культури з акцентом на дотримання процедур, ієрархію, контроль до більш гнучкої, інноваційної культури, що заохочує експериментування, горизонтальну комунікацію, швидке прийняття рішень. Трансформація від культури конкуренції між відомствами за ресурси, вплив, визнання до культури співпраці, де успіх вимірюється колективними результатами екосистеми.

Поетапне впровадження екосистемного підходу має враховувати обмеженість ресурсів, інституційні обмеження, необхідність демонстрації швидких результатів для створення політичної підтримки та інституційного імпульсу. Перший етап фокусується на створенні пілотних проектів у найкритичніших сферах, де потреба у координації найбільш очевидна та гостра, а потенційні вигоди від інтеграції можуть бути продемонстровані швидко. Прикладами можуть бути інтегрована система захисту енергетичної інфраструктури від кібератак, що об'єднує операторів мереж, кіберполіцію, спецслужби, приватні компанії з кібербезпеки, або платформа для виявлення та протидії дезінформаційним кампаніям, що інтегрує моніторинг соціальних медіа, фактчекінг, стратегічні комунікації. Швидкі перемоги – демонстрація конкретних успіхів пілотів, таких як запобігання серйозній кібератаці або ефективне спростування дезінформації – створюють політичну підтримку, переконують скептиків у цінності підходу, мотивують інші агенції приєднатися [1].

Другий етап передбачає горизонтальне масштабування перевірених моделей на інші сектори критичної інфраструктури та типи загроз. Успішні практики координації, протоколи обміну інформацією, технологічні рішення, що довели ефективність у пілотах, адаптуються та впроваджуються у фінансовому секторі, транспорті, охороні здоров'я, системі виборів. Створюються галузеві екосистеми з специфічними для кожного сектору учасниками, загрозами, технологіями, але інтегровані через спільні стандарти та платформи для забезпечення загальної ситуаційної обізнаності.

Третій етап фокусується на вертикальній інтеграції різних рівнів системи – від операційного рівня реагування на конкретні інциденти через тактичний рівень аналізу кампаній до стратегічного рівня оцінки довгострокових трендів та формування політики – у єдину багаторівневу екосистему. Це вимагає створення ієрархії платформ з різним рівнем абстракції, механізмів агрегації інформації знизу вгору та декомпозиції стратегічних цілей зверху вниз.

Четвертий етап передбачає поглиблену міжнародну інтеграцію та створення транскордонних екосистем безпеки з союзниками та партнерами. Це особливо

актуально у контексті європейської інтеграції України, де очікується адаптація до стандартів ЄС у сфері кібербезпеки, участь у спільних європейських ініціативах, таких як European Cyber Security Organisation, інтеграція у системи обміну інформацією НАТО. На цьому етапі національна екосистема стає вузлом у глобальній мережі екосистем, що обмінюються інформацією, координують відповіді на транснаціональні загрози, спільно розробляють нові спроможності [6].

Кібербезпека самої екосистеми вимагає особливої уваги на всіх етапах формування та функціонування. Парадокс полягає в тому, що система, створена для захисту від загроз, сама стає привабливою ціллю для атак, причому скомпрометування екосистеми може мати катастрофічні наслідки через концентрацію критичної інформації та взаємозв'язок компонентів. Необхідні багатошарові механізми захисту: мережева сегментація для ізоляції критичних компонентів та обмеження поширення атак, наскрізне шифрування даних як у спокої так і при передачі, багатофакторна автентифікація для доступу до систем, постійний моніторинг аномалій та підозрілої активності через SIEM системи, регулярне тестування на проникнення командами етичних хакерів для виявлення вразливостей, плани реагування на інциденти з чіткими процедурами, ролями, комунікаціями, регулярні навчання персоналу кібергігієні [7]. Особливу увагу необхідно приділити захисту ланцюгів постачання програмного та апаратного забезпечення від імплантації закладок, верифікації цілісності компонентів, використанню довірених постачальників.

Український контекст ставить специфічні виклики та створює унікальні можливості для формування цифрової екосистеми національної безпеки. Виклики включають: необхідність функціонування в умовах активного повномасштабного конфлікту, коли системи піддаються постійним інтенсивним кібератакам, дезінформаційним кампаніям, фізичним руйнуванням інфраструктури; обмеженість фінансових та людських ресурсів порівняно з державою-агресором, яка володіє значно більшим бюджетом, технологічною базою, кількістю фахівців; наявність великої кількості застарілих систем та процесів, що потребують модернізації, але повна заміна яких неможлива через вартість та час; інституційні бар'єри, включно з бюрократією, корупційними ризиками, відомчою конкуренцією, застарілим законодавством; втрату частини території внаслідок окупації з розташованими там об'єктами інфраструктури, персоналом, даними.

Водночас Україна володіє рядом унікальних можливостей. По-перше, це високий рівень цифровізації українського суспільства створює сприятливе середовище для цифрових ініціатив – за даними міжнародних рейтингів Україна входить до топ-50 країн за рівнем цифрового розвитку, успіх платформи «Дія» демонструє готовність громадян до використання цифрових послуг. По-друге, це потужний ІТ-сектор з приблизно 200,000 фахівців володіє експертизою світового рівня у розробці програмного забезпечення, штучному інтелекті, кібербезпеці та демонструє високу готовність до співпраці у сфері національної безпеки. По-третє, це унікальний досвід протидії гібридним загрозам, накопичений за десятиліття конфлікту – від кібератак на критичну інфраструктуру 2015-2017 років через дезінформаційні кампанії до повномасштабного вторгнення – створив експертизу, яка є цінною не лише для України, а й для міжнародних

партнерів. По-четверте, це потужна міжнародна підтримка від США, ЄС, Великої Британії та інших партнерів через програми технічної допомоги, трансферу технологій, навчання, фінансування. По-п'яте, це високий рівень мобілізації громадянського суспільства та волонтерського руху, готовність громадян активно долучатися до протидії загрозам.

Успішні українські кейси ілюструють потенціал екосистемного підходу навіть в умовах обмежених ресурсів та активного конфлікту. Платформа «Дія» продемонструвала можливість швидкої масштабної цифровізації через централізовану платформу, що інтегрує понад 120 державних послуг, об'єднує десятки відомств, має понад 20 мільйонів користувачів, і хоча первинно створена для цивільних послуг, її архітектура та досвід міжвідомчої інтеграції застосовні для безпекової сфери. CERT-UA як національна команда реагування на кіберінциденти ефективно координує взаємодію між державними органами, приватним сектором, міжнародними партнерами у відповідях на кібератаки, обміні інформацією про загрози, попередженні про вразливості, демонструючи можливості горизонтальної координації. IT Army – волонтерська ініціатива, що об'єднала тисячі IT-фахівців для проведення кібероперацію проти агресора – ілюструє потенціал залучення громадянського суспільства, хоча й ставить складні питання контролю, відповідальності, міжнародного права. Ініціативи верифікації інформації, такі як StopFake, VoxCheck та інші, що залучають громадянських журналістів, технологічні компанії, академічні інституції для виявлення та спростування дезінформації, демонструють можливості багатостороннього партнерства.

Міжнародний досвід також надає цінні уроки для формування української екосистеми. Так, Ізраїль створив одну з найбільш ефективних екосистем безпеки через тісну інтеграцію між армією, розвідувальними службами, академічними інституціями та приватним сектором, що підживлюється системою обов'язкової військової служби з акцентом на технологічні підрозділи, культурою інновацій та підприємництва, державною підтримкою стартапів у сфері безпекових технологій через програми на кшталт BIRD Foundation [9]. Ізраїльський досвід показує важливість інституціоналізації циркуляції талантів між армією, де молодь отримує передову технічну підготовку та досвід роботи з реальними загрозами, університетами, що проводять передові дослідження, та стартапами, що комерціалізують технології.

Естонія після масованих кібератак 2007 року, які паралізували значну частину інфраструктури країни, побудувала одну з найбільш стійких цифрових екосистем через принцип розподіленої архітектури без єдиних точок відмови, створення Data Embassy – резервних копій критичних даних, розміщених за кордоном, активне міжнародне партнерство, включно з розміщенням на своїй території Cooperative Cyber Defence Centre of Excellence НАТО [17]. Естонський досвід демонструє можливості малої країни створити світового рівня спроможності через фокусування на специфічній ніші, залучення міжнародних партнерів, інвестиції у освіту та дослідження.

Сполучені Штати розвивають екосистему кібербезпеки через спеціалізовану агенцію CISA (Cybersecurity and Infrastructure Security Agency), що виконує функ-

ції національного координатора між федеральним урядом, урядами штатів, приватним сектором, координує реагування на великі інциденти, надає рекомендації, проводить навчання. Американський досвід показує важливість наявності організації з чітким мандатом на координацію, достатніми ресурсами та повноваженнями, але без прямого оперативного контролю над учасниками, що дозволяє балансувати централізовану координацію з децентралізованою реалізацією [4].

Сінгапур через ініціативу Smart Nation демонструє можливості централізованого стратегічного планування цифрової трансформації при збереженні важливої ролі приватного сектору у реалізації, створення спеціальної урядової структури Smart Nation and Digital Government Office для координації, значних інвестицій у цифрову інфраструктуру, R&D, освіту [20]. Сінгапурський досвід показує, що навіть авторитарніші моделі governance можуть бути ефективними у створенні технологічних спроможностей, хоча виникають питання балансу з демократичними цінностями, правами людини.

Висновки з даного дослідження і перспективи подальших досліджень. Таким чином, формування цифрової екосистеми національної безпеки є необхідною та невідворотною відповіддю на фундаментальні виклики, які гібридні загрози створюють для традиційних моделей організації безпекових систем. Гібридні загрози за своєю природою є багатовимірними, динамічними, транскордонними, що вимагає інтеграції різнорідних акторів, технологій, інформації, аналітичних спроможностей та процесів у єдину систему, здатну функціонувати у режимі, наближеному до реального часу. Традиційна ієрархічна модель з відомчою фрагментацією, обмеженим обміном інформацією, повільними процесами координації є структурно неадекватною для протидії таким загрозам. Екосистемний підхід, що базується на горизонтальній інтеграції через цифрові платформи, мережевій архітектурі взаємодії, розподіленій аналітиці при збереженні організаційної автономії учасників, пропонує більш адаптивну, стійку та ефективну альтернативну модель.

Розроблена у дослідженні концептуальна модель цифрової екосистеми національної безпеки базується на п'яти взаємопов'язаних функціональних шарах: інформаційно-аналітична інфраструктура для збору та первинної обробки даних з різнородних джерел, технологічна платформа, що інтегрує штучний інтелект, великі дані, блокчейн та інші передові технології, аналітичні інструменти для трансформації даних у дієву інформацію, процесні механізми координації та протоколи взаємодії, система управління та governance для забезпечення узгодженості дій. Ефективність екосистеми визначається не лише спроможностями окремих компонентів, а критично залежить від якості їх інтеграції, щільності та надійності зв'язків між учасниками, ефективності механізмів координації.

Формування екосистеми вимагає вирішення комплексу взаємопов'язаних викликів. Технічні виклики включають забезпечення реальної інтероперабельності різнорідних систем, кібербезпеку платформ, обробку великих обсягів даних у реальному часі, інтеграцію застарілих систем з новими технологіями. Інституційні виклики охоплюють створення адекватної нормативно-правової бази для обміну даними при дотриманні прав людини, подолання відомчих бар'єрів та культури інформаційних силосів, розробку ефективних моделей

державно-приватного партнерства, узгодження стимулів різних учасників. Культурні виклики стосуються трансформації організаційної культури від бюрократичної до інноваційної, від конкуренції до співпраці, розвитку цифрових компетенцій персоналу, формування міжвідомчої довіри.

Перспективи подальших досліджень включають низку важливих напрямів. По-перше, необхідні емпіричні дослідження ефективності різних конфігурацій екосистем через порівняння об'єктивних показників: час від виявлення загрози до реагування, точність прогнозів систем раннього попередження, відсоток успішно відбитих атак, вартість інцидентів. По-друге, важливими є дослідження механізмів довіри між учасниками екосистеми та їх впливу на готовність до обміну інформацією, оскільки довіра є критичним, але складно вимірюваним фактором. По-третє, потребують поглибленого аналізу етичні дилеми використання штучного інтелекту у безпеці та розробка нормативних рамок, що балансують ефективність та права людини. По-четверте, корисною була б розробка методології оцінки зрілості цифрових екосистем національної безпеки для самодіагностики та бенчмаркінгу.

Стаття надійшла до редакції 15.09.2025
Стаття рекомендована до друку 16.10.2025
Опубліковано 30.12.2025

Viacheslav Dziundziuk, doctor of science in public administration, professor,
Head of Public Policy Chair, Educational and Scientific Institute «Institute of Public Administration»,
V. N. Karazin Kharkiv National University, 4 Svobody Sq., Kharkiv, 61022, Ukraine
ORCID ID: https://orcid.org/0000-0003-0622-2600 e-mail: vbdzun@gmail.com

FORMING A DIGITAL NATIONAL SECURITY ECOSYSTEM TO COUNTER HYBRID THREATS

Abstract. Hybrid threats, which combine military, informational, cyber, economic and diplomatic tools of influence, constitute one of the most serious challenges to national security in the 21st century. Traditional models of security system organization, built on principles of departmentalization and vertical hierarchy, demonstrate limited effectiveness in countering threats that are inherently multidimensional, dynamic and transborder. Ukraine's experience, which has been resisting large-scale hybrid aggression since 2014, demonstrates the critical need to integrate diverse security actors, technologies and processes into a unified digital ecosystem capable of ensuring synergetic effect in detecting, analyzing and neutralizing threats. The article aims to develop a conceptual model of a digital national security ecosystem and identify key principles, architectural solutions and institutional mechanisms for its formation under conditions of hybrid warfare.

The article substantiates that an effective digital national security ecosystem should be based on five interconnected components: information-analytical infrastructure for collecting and processing data from diverse sources; technological platform integrating artificial intelligence, big data, blockchain and cybersecurity tools; analytical instruments for transforming data into actionable information; process mechanisms for coordination and

decision-making; governance system defining rules of interaction between state, private and civil society actors. Each component performs specific functions, but their effectiveness is achieved only through tight integration and interaction.

Analysis of international experience shows that the most effective ecosystems are characterized by a balance of centralized coordination and decentralized initiative, combination of state regulation and market competition, integration of technological capabilities and institutional mechanisms of trust. Israeli model demonstrates advantages of tight integration between defense sector, academia and private business. Estonian model shows effectiveness of distributed architecture and international partnership. American experience underscores importance of specialized coordination agencies. Singapore practice illustrates possibilities of centralized planning while preserving private sector role.

Ukrainian context presents specific requirements for ecosystem formation: necessity to function under active conflict conditions, limited resources, presence of legacy systems and institutional barriers, high corruption risks. Simultaneously, Ukraine possesses significant opportunities: powerful innovative potential of IT sector with world-class expertise and readiness for cooperation, unique experience of countering hybrid threats accumulated over decade of conflict, international support from partners, high level of civil society mobilization. Recommendations are formulated for phased implementation of ecosystem approach with prioritization of critical functions, use of quick wins to create institutional momentum, ensuring multilayer cybersecurity and competence development at all transformation stages.

Keywords: *public administration, digital ecosystem, national security, hybrid threats, interagency coordination, artificial intelligence, cybersecurity, digital transformation, public-private partnership.*

In cites: Dziundziuk, V. B. (2025). Forming a digital national security ecosystem to counter hybrid threats. *Theory and Practice of Public Administration*, 2 (81), 315–330. http://doi.org/10.26565/1727-6667-2025-2-19 [in Ukrainian].

REFERENCES:

1. Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. *Journal of Management*, 43(1), 39–58. DOI: https://doi.org/10.1177/0149206316678451
2. Ansell, C., & Gash, A. (2018). Collaborative platforms as a governance strategy. *Journal of Public Administration Research and Theory*, 28(1), 16–32. DOI: https://doi.org/10.1093/jopart/mux030
3. Berzins, J. (2020). The theory and practice of new generation warfare: The case of Ukraine and Syria. *Journal of Slavic Military Studies*, 33(3), 355–380. DOI: https://doi.org/10.1080/13518046.2020.1824109
4. Bryson, J., Crosby, B., & Stone, M. (2015). Designing and implementing cross-sector collaborations: Needed and challenging. *Public Administration Review*, 75(5), 647–663. DOI: https://doi.org/10.1111/puar.12432
5. Buchanan, B. (2020). The AI Triad and What It Means for National Security Strategy. Washington: Center for Security and Emerging Technology. DOI: https://doi.org/10.51593/20200021
6. Coaffee, J., & Lee, P. (2016). Urban resilience: Planning for risk, crisis and uncertainty. London: Palgrave Macmillan. URL: http://www.macmillanihe.com/t/9781137288820/

7. Dunn C. M. (2018). Cybersecurity in Switzerland. Zurich: Springer International Publishing. DOI: https://doi.org/10.1007/978-3-319-10620-5

8. Gil-Garcia, J., Dawes, S., & Pardo, T. (2018). Digital government and public management research: Finding the crossroads. *Public Management Review*, 20(5), 633–646. DOI: https://doi.org/10.1080/14719037.2017.1327181.

9. Hoffman, F. (2007). Conflict in the 21st century: The rise of hybrid wars. Arlington: Potomac Institute for Policy Studies, 72. URL: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf

10. Jackson, W. (2019). Cybersecurity ecosystem: Building collaboration for resilience. Cambridge: MIT Press. URL: https://rlj0713.medium.com/cybersecurity-an-introduction-630cc8a9ba8d

11. Jacobides, M., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, 39(8), 2255–2276. DOI: https://doi.org/10.1002/smj.2904

12. Janowski, T. (2015). Digital government evolution: From transformation to contextualization. *Government Information Quarterly*, 32(3), 221–236. DOI: https://doi.org/10.1016/j.giq.2015.07.001

13. Klievink, B., Bharosa, N., & Tan, Y. (2016). The collaborative realization of public values and business goals: Governance and infrastructure of public–private information platforms. *Government Information Quarterly*, 33(1), 67–79. DOI: https://doi.org/10.1016/j.giq.2015.12.002

14. Lanoszka, A. (2016). Russian hybrid warfare and extended deterrence in eastern Europe. International Affairs, 92(1), 175–195. DOI: https://doi.org/10.1111/1468-2346.12509

15. Margetts, H., & Dunleavy, P. (2013). The second wave of digital-era governance: A quasi-paradigm for government on the Web. *Philosophical Transactions of the Royal Society A*, 371(1987), 20120382. DOI: https://doi.org/10.1098/rsta.2012.0382

16. Moore, J. (1993). Predators and prey: A new ecology of competition. *Harvard Business Review*, 71(3), 75–86. URL: https://www.researchgate.net/publication/13172133_Predators_and_Prey_A_New_Ecology_of_Competition

17. Renz, B., & Smith, H. (2016). Russia and hybrid warfare: Going beyond the label. Helsinki: Aleksanteri Institute. URL: https://helda.helsinki.fi/server/api/core/bitstreams/9514b166-0249-42a4-a408-9195e7d32292/content

18. Shelest, Hanna (2015) After the Ukrainian crisis: Is there a place for Russia? *Southeast European and Black Sea Studies*, 15:2, 191-201. DOI: https://doi.org/10.1080/14683857.2015.1060019

19. Stoker, D. (2019). Why America loses wars: Limited war and US strategy from the Korean War to the present. Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/9781108611794

20. Vespignani, A. (2012). Modelling dynamical processes in complex socio-technical systems. *Nature Physics*, 8(1), 32–39. DOI: https://doi.org/10.1038/nphys2160

21. Wilson, A. (2014). Ukraine crisis: What it means for the West. New Haven: Yale University Press, 236. DOI: https://doi.org/10.1017/nps.2019.20

The article was received by the editors 15.09.2025
The article is recommended for printing 16.10.2025
Published 30.12.2025