Відбудувати краще:

як Україна обирає цифрову архітектуру майбутнього

ТЕМА НОМЕРА

Відбудувати «краще» означає не відтворити стару цифрову модель, а сформувати нову архітектуру майбутнього: держава задає зрозумілі правила гри, ринок забезпечує інженерну спроможність і масштабування, а цифровий суверенітет перетворюється з політичного лозунгу на щоденну практику управління, безпеки та розвитку.

Лютий 2022-го. 72 години. Критичні державні реєстри — в хмарі. Країна не зупинилась завдяки інженерам, архітекторам, адміністраторам серверів. Без урочистих наказів і пресрелізів. Чотири роки потому ці ж люди будують цифрову державу — серед руїн і під ракетами. І досі чекають відповіді: вони критичні чи ні. **Не теоретично. Юридично.** За критерієм функції, а не за назвою компанії у переліку КМУ. Питань у 2026-му більше, ніж було у 2022-му. Тоді — одне: вижити. Тепер — яку цифрову архітектуру обирати, з ким будувати і чи встигнемо зайняти місце у цифровій Європі. Польща — наш партнер, але водночас головний конкурент за роль регіонального цифрового ядра — вже обирає. Тим часом ЄС формує EuroStack — власний технологічний стек, де суверенна хмарна сертифікація EUCS стане фільтром доступу до спільного ринку. Місця розподіляються вже зараз.

Де стоїть Україна: картина без ретуші

Перш ніж говорити про Ізраїль, Естонію і Польщу та порівнювати з ними — варто чесно відповісти на простіше запитання: де зараз стоїть Україна? Не де хотіла б. Де є — станом на 2026-й (**таблиця 1**). Відповідь не чорно-біла. Є чим пишатися, але є й те, що турбує. І обидва ці відчуття майже по кожному з вимірів, чи то посилення кібербезпеки або людський фактор — цілком реальні. Розглянемо декілька з них.

Кадри. Пишаємось українськими експертами, саме вони тримають IT-сектор. За даними Lviv IT Cluster (IT Research Ukraine 2025), в Україні зараз 245 000 IT-фахівців — на 2,9% більше, ніж рік тому. Кількість тих, хто за кордоном, скоротилася до 58 000: мінус 10% порівняно з 2024-м. Загальний реєстр галузі — 303 000 фахівців

Таблиця 1. Шість вимірів цифрової стійкості України — 2026

Вимір	Стан	Оцінка*	Ключова лакуна
Фізична мережа	Відновлюється, доступність >90%	7/10	Концентрація на 4–5 хабах, вразливість магістралей
Хмари й обчислення	De Novo та GigaCloud + AWS/AzureGov	6/10	EUCS-сертифікація нац. провайдерів
Кіберзахист	CERT-UA + NIS2 через DRS2UA	7/10	Перехід від реактивної до проактивної моделі
Цифрове врядування	«Дія» + Трембіта 2.0 (у процесі)	7/10	Повна інтеграція реєстрів; закон про цифрове посольство
Кадри	303 000 всього / 245 000 у країні; 39% без бронювання	6/10	Системний захист інфраструктурного сегмента
Інвестклімат	DT4UA + донори; приватний капітал — слабко	5/10	Правові гарантії; перший гіперскейлер-якір

* Оцінки виставлені редакційною аналітичною групою МтБ на основі відкритих даних регуляторів, галузевих асоціацій та DOU (2025). Кожен вимір оцінювався за трьома параметрами: наявність правової бази, операційна готовність і відповідність міжнародним стандартам. Шкала: реалізовано (8–10) / частково (6–7) / потребує рішення (5) / критично відсутнє (1–4).Більшість позицій — «частково» або «потребує рішення». Це не катастрофа. Але й не підстава зачекати — бо вікно для дій не стоїть.

(245 000 у країні + 58 000 за кордоном). IT-ринок сягнув $7,48 млрд, IT-експорт — $6,45 млрд (Lviv IT Cluster, IT Research Ukraine 2025; за підсумками 2024 р.). Сектор не просто вижив. Він повернувся до зростання.

Однак ці цифри не показують повної картини. Якщо у грудні 2025 року (за даними DOU) 39% українських IT-спеціалістів не мали бронювання, то після 30 травня 2026 року ситуація суттєво погіршилася. Із ухваленням Постанови КМУ №692 проблема перейшла у нову площину: відтепер ризики виникають не лише для незабронюваних працівників, а й для тих, хто вже має цей статус. З 1 вересня 2026 року зарплатний поріг для забронюваного працівника зростає з коефіцієнта 2,5 до 3,0 мінімальних зарплат — 25 941 грн на місяць (КМУ Постанова №692, 30.05.2026; виняток становлять резиденти Дія.City та прифронтові підприємства). Паралельно всі рішення про статус «критично важливого підприємства» — включно з IT-компаніями, cloud-операторами і системними інтеграторами — підлягають обов'язковому перепідтвердженню до 1 вересня 2026 року. Хто не доведе відповідність новим критеріям — втрачає право бронювати автоматично.

«Дія» і Трембіта 2.0: фасад і фундамент. «Дія» — 20+ мільйонів активних користувачів, сотні держсервісів в одному застосунку. Блискучий фронтенд. Але «Дія» залежить від бекенду: наскільки злагоджено обмінюються даними реєстри. Трембіта 2.0 — саме ця магістраль. Розгортання триває. Кількість повністю інтегрованих реєстрів досі не є публічною цифрою — і це само по собі тривожний сигнал.

«Дія» — це довіра громадянина до держави. Трембіта 2.0 — довіра всередині держави. Перше без другого — гарний фасад на хиткому фундаменті.

Українська цифрова відбудова у 2026 році вже не є лише проєктом майбутнього. Дія.City, Дія.Engine, Дія.Бізнес і сервіси відкритих даних — це вже не фасад послуг, а операційний контур сервісної держави, яка збирає власну інфраструктурну лінію, де кожен сервіс стає частиною єдиної системи, а не окремим проєктом.

Три уроки без мотиваційних плакатів

Порівнювати Україну з успішними країнами легко. Корисно — значно рідше. Коли порівняння зводиться до «вони змогли — і ми зможемо» — це не аналіз. Це мотиваційний плакат із гарними цифрами.

Ізраїль, Естонія і Польща цікаві не як зразки для натхнення — а як відповіді на конкретні запитання, з якими Україна стикається сьогодні (**таблиця 2**). Три рівні — три різні виміри стійкості. Кожен є умовою для наступного: без операційної витривалості неможливо реалізувати архітектурний задум; без архітектурного фундаменту — залучити стратегічні інвестиції.

Таблиця 2. Модель адаптації міжнародного досвіду для цифровізації та безпеки України

Рівень	Питання для України	Країна	Ключовий крок	Горизонт
Операційний	Як захистити те, що є — просто зараз?	Ізраїль	Кіберзахист як державна доктрина, не відомча функція	Сьогодні
Архітектурний	Як побудувати державу, що виживе без фізичної території?	Естонія	Держава як платформа, а не набір застосунків	Завтра
Стратегічний	Як залучити ресурси масштабу для якісного стрибка?	Польща	Регуляторна передбачуваність як магніт для капіталу	Післязавтра

КИЇВЩИНА ЯК МАЙДАНЧИК НОВОЇ ЦИФРОВОЇ ВІДБУДОВИ

Київщина має стати регіоном, де відбудова не повторює старі помилки, а одразу задає нову планку. Ми були серед перших, хто відчув масштаб руйнувань, тому сьогодні наше завдання – не просто відновити втрачене, а показати, як поєднати стійкість, безпеку і сучасні цифрові рішення на рівні області та громад. Бородянка вже є прикладом того, що відбудова краще, ніж було, може бути не гаслом, а практикою: від житлової відбудови до нових підходів у транспорті, цифрових сервісах і безбар'єрності.

Максим СТОЛЯРЧУК,
заступник голови Київської ОДА з питань цифрового розвитку

У цифровій інфраструктурі нам потрібна комбінована модель: хмара там, де вона дає масштаб і швидкість, локальна інфраструктура там, де критичними є безпека й контроль. Але головне – це люди. Кіберфахівці, мережеві інженери, DevSecOps-спеціалісти й архітектори цифрових рішень мають бути захищені так само, як і сама інфраструктура, бо саме вони тримають її в робочому стані. Київщина має бути не просто регіоном відновлення, а регіоном, який показує Україні робочу модель цифрової відбудови.

Ізраїль: кіберзахист як доктрина, а не відомча функція

Ізраїльська кіберіндустрія виглядає ззовні як набір дивовижних цифр. Хайтек — 57–58% усього експорту. Стартапи у 2025-му залучили $15,6 млрд. Але якщо дивитися тільки на цифри — найважливіше залишається поза кадром.

Найважливіше — це **Національна кібердирекція Ізраїлю (INCD)**, яка у лютому 2025-го ухвалила нову Стратегію кібербезпеки (INCD, «National Cyber Strategy», 2025). Ключова зміна — не технічна, а концептуальна. Попередня стратегія розглядала кіберпростір як джерело національної могутності. Нова — як умову функціонування критичних процесів держави. Різниця в одне слово — і в повністю іншій архітектурі інститутів.

INCD — не «CERT на стероїдах», а структура при Канцелярії Прем'єр-міністра Ізраїлю з прямим координаційним зв'язком з Радою національної безпеки, яка регулює ринок, аналізує загрози і є стратегічним партнером для приватного сектору. У 2025-му вона надіслала 2304 проактивних попередження (з 2480 загальних) організаціям — не після атаки, а до неї (INCD Annual Report, 2025). Це і є «активна безпека» в дії.

Після 7 жовтня 2023-го 15–20% ізраїльських IT-фахівців опинилися в резерві (Israel Tech Policy Institute) — дзеркало українського виклику. Ізраїльська система бронювання технологічних кадрів будувалась десятиліттями через структури на кшталт Unit 8200; після 7 жовтня вона пройшла реальне бойове випробування. Логіка незмінна: без цих людей держава — як укріплення без гарнізону.

Питання до України. *Де аналог INCD — об'єднаний центр, що поєднує регулювання, аналітику загроз і проактивне попередження на рівні всього уряду?*

ХТО БУДУЄ АРХІТЕКТУРУ КІБЕРЗАХИСТУ

В Україні архітектура кіберзахисту не зводиться до одного центру чи однієї інституції. РНБО задає стратегічну рамку, ДССЗЗІ формує політики захисту, CERT-UA реагує на інциденти, СБУ захищає державні ресурси, кіберполіція розслідує злочини, НБУ окремо відповідає за фінансовий сектор, а Міністерство оборони має власну зону відповідальності. Галузеві центри кібербезпеки далі впроваджують ці політики у своїх сферах. CERT-UA при цьому функціонує в складі Держспецзв'язку і залишається однією з опор державної моделі реагування.

Сергій БОБРОВ,
технічний директор,
«ЕС ЕН ТІ УКРАЇНА»

Тому питання не в тому, чи є в Україні аналог INCD, а в тому, як працює розподілена модель, де кожен рівень не дублює, а посилює інший. Приватний сектор у цій конструкції має бути не лише об'єктом захисту, а й співучасником оборони – через власні продукти, аналітику, MSSP-сервіси та постійну взаємодію з державою. Саме так і будується реальна кібероборонна архітектура країни.

Естонія: держава як платформа, а не набір застосунків

Про Естонію прийнято говорити у захопленому тоні. Але захоплення — поганий аналітичний інструмент. Воно спрощує.

Естонія не будувала «е-уряд» у звичному розумінні — цифровий фасад поверх паперових процесів. Вона створила інфраструктурний фундамент, де дані рухаються між інституціями самостійно, громадянин надає їх один раз, а держава не «губить» факти через відпустку чиновника.

В основі — **X-Road**, децентралізована платформа обміну між реєстрами, запущена у 2001 році (e-Estonia Briefing Centre). Кожна транзакція — з криптографічним підтвердженням цілісності. Жоден запис не можна відредагувати без сліду. Ефект: щорічна економія понад 1400 років адміністративного робочого часу (RIA Annual Report). Так, 1400 років. Це не помилка.

У 2017-му Естонія відкрила **«цифрове посольство»** у Люксембурзі — перша держава у світі, яка вивела копії критичних реєстрів за межі власної території із закріпленою екстериторіальною юрисдикцією: естонське право поширюється на ці дані незалежно від фізичного місцезнаходження (Estonian Riigikogu, 2017). Логіка проста і безжальна: якщо ворог окупує Таллінн — держава функціонуватиме далі.

Хмарна евакуація реєстрів України у 2022-му — правильна відповідь. Але це було зроблено «на ходу». «Цифрове посольство» — інша якість: юридично визначений статус, постійна синхронізація незалежно від воєнної кон'юнктури чи корпоративної політики AWS.

Естонська модель будувалася 20+ років для країни з населенням 1,4 млн. Відстань між Трембітою 2.0 і X-Road — це не рядки коду, а кількість реєстрів, повністю інтегрованих в єдину систему. Ця відстань скорочується. Але темп залежить від волі, а не від технічних можливостей.

Питання до України. *Де зберігаються найважливіші державні дані у разі найгіршого сценарію — і чи є правовий механізм, аналогічний* ***Data Embassies Act*** *(естонський закон 2017 р. про екстериторіальну юрисдикцію для держданих, що зберігаються за кордоном)? Станом на 2026 рік — немає.*

Польща: регуляторна передбачуваність як стратегічний капітал

Польща — найближчий і найпровокативніший приклад. Провокативний — бо ставить незручне запитання: якщо це можливо в Польщі (роль регіонального цифрового ядра ЦСЄ), чому не відбувається в Україні? Відповідь — не «тому що війна», а завдяки чітким послідовним діям. Польський шлях стартував задовго до 2022-го.

У 2019–2020 роках, коли Microsoft ухвалювала рішення про Azure Poland Central — перший власний датацентровий кампус гіперскейлера в ЦСЄ, — польська відповідь була конкретною: ось правова рамка, ось захист інвестицій, ось університетський кластер. Діалог тривав 18 місяців (Warsaw

Institute for Digital Policy). Перший якір — і пішов ланцюговий ефект. У межах ініціативи **EuroStack** — концепції повного технологічного стеку під європейським контролем — Польща прагне стати одним із центральних вузлів (**таблиця 3**):

Таблиця 3. Інвестиції у цифрову інфраструктуру Польщі

Рік	Подія	Обсяг інвестицій
2020	Microsoft: план цифрової трансформації Польщі та створення першого датацентрового регіону Microsoft Cloud у Польщі	$1 млрд
2025	Microsoft: розширення хмарної та AI-інфраструктури	≈ $704 млн
2023 –2025	Intel: анонс заводу складання й тестування чипів біля Вроцлава; проєкт скасовано у 2025 р.	до $4,6 млрд, скасовано
2025	PIAST-AI Factory у Познані, проєкт EuroHPC / EU AI Factories	€100 млн, 50% ЄС + 50% держбюджет

Загальна сума діючих зобов'язань — $1,8 млрд (без скасованого проєкту Intel на $4,6 млрд). Для порівняння: весь IT-експорт України — $6,45 млрд (IT Research Ukraine 2025). Але природа цих грошей різна: Польща залучила капітальні інвестиції в «залізо» і датацентри — Україна заробила на продажі послуг. Прямі вкладення в цифрову інфраструктуру України за той самий період — не більше $200–300 млн (оцінка редакції МтБ на основі відкритих даних Prozorro і публічних звітів операторів) — різниця на порядок.

Хоча треба розуміти, що прихід гіперскейлерів не гарантує незалежності у цифровому просторі. Azure Poland Central зберігає дані в Польщі — але моделі, чипи і алгоритми залишаються американськими. Тому Польща тепер прагне стати повноправним власником через PIAST і Gaia AI Factory. Для України це дороговказ: закласти власний AI-стек як частину першої якірної угоди одразу, а не «потім».

Питання для України. *Польща — партнер чи конкурент за роль регіонального цифрового ядра? Україна може стати частиною цієї архітектури — але лише якщо сформує власні умови входу, а не чекатиме на чужі.*

Після вивчення досвіду різних країн у розвитку національної цифрової інфраструктури і кібербезпеки постає питання: що в цьому напрямку може зробити Україна вже зараз, не чекаючи завершення війни чи реформ?

Цифровий суверенітет як основа майбутньої IT-архітектури України

І поки на державному рівні наразі немає чітких відповідей на наші «Питання до України», паралельно український приватний ринок переходить від оборонної позиції до коаліційної моделі. Одним із прикладів такого підходу є діяльність **DSUA** — Українського альянсу цифрового суверенітету.

Головна ідея DSUA полягає в тому, щоб важливі державні, медичні, фінансові та оборонні дані зберігалися й оброблялися в Україні, відповідно до українського законодавства. Це стало особливо важливим у воєнних умовах, коли частина цифрових ресурсів залежить від іноземної інфраструктури.

Альянс демонструє, що цифрове майбутнє України має будуватися не лише на інтеграції з глобальними технологіями, а й на розвитку власних хмарних сервісів, датацентрів, стандартів безпеки та національних експертних знань і досвіду. Так, у квітні 2026 року DSUA взяв участь у Sovereign Tech Europe в Брюсселі, де цифровий суверенітет був однією з основних тем. Це свідчить про те, що українські хмарні провайдери прагнуть співпрацювати з європейськими партнерами на рівних, формуючи спільні підходи до безпеки даних і сервісів.

ТЕРМІНОЛОГІЧНИЙ ДОВІДНИК

EUCS	EU Cloud Cybersecurity Scheme — схема сертифікації хмарних послуг (ENISA) для ринку ЄС
EuroStack	Ініціатива ЄС з створення незалежного технологічного стеку — від чипів до хмарних платформ — під європейським контролем
INCD	Israel National Cyber Directorate — Національна кібердирекція Ізраїлю
X-Road	Естонська платформа захищеного обміну даними між держреєстрами — основа «держави як платформи»
NIS2	EU Network and Information Security Directive 2 — директива ЄС з кібербезпеки для критичних секторів
DRS2UA	Digital Resilience Strategy of Ukraine — Стратегія цифрової стійкості України, аналог NIS2 для UA-контексту
Data Embassies Act	Естонський закон 2017 р. про екстериторіальну юрисдикцію для держданих, що зберігаються за кордоном

ПОЛЬЩА НЕ РОБИТЬ НАС «СУБПРОВАЙДЕРОМ»

Кирило НАУМЕНКО,
CTO GigaCloud

Польща дійсно стала важливим cloud-хабом регіону після запуску Azure Poland Central, але я б не дивився на це як на сценарій, у якому українські оператори автоматично стають «супутниками» польського ринку. Україна вже має власних сильних cloud-гравців, enterprise-експертизу, датацентри та великий досвід роботи зі складною інфраструктурою. Тому на горизонті 3–5 років я скоріше бачу модель партнерської інтеграції з hyperscaler-екосистемами, а не втрату суб'єктності локального ринку. Наявність hyperscaler-регіонів у Польщі – це скоріше плюс для клієнтів, оскільки дозволяє будувати більш гнучкі hybrid– та multi-cloud-рішення.

Частина workloads дійсно буде оптимально працювати через глобальні платформи, але при цьому залишатиметься великий сегмент задач, де критично важливими будуть локальна присутність, контроль над даними, sovereign-підхід та compliance-вимоги. Саме тому я не думаю, що майбутнє українського cloud-ринку – це роль «субпровайдера». Скоріше мова йде про формування власного сильного regional cloud market з інтеграцією у європейську цифрову екосистему.

УКРАЇНСЬКА ВЕРСІЯ ЦИФРОВОГО СУВЕРЕНІТЕТУ, АБО ЧОМУ ЗА 5 РОКІВ МИ МОЖЕМО СТАТИ «ЧУЖИМИ» ДЛЯ ЄВРОПИ (джерело: блог компанії De Novo)

Ситуація в Україні подібна до європейської, але з вітчизняним колоритом. Історично ми ніколи не мали довгих стратегій: наш принцип – «бери більше, кидай далі до наступного повороту». Проте запит на цифрову суверенізацію зростає. У цьому сенсі Україна – це Європа, тільки бідна, воююча та побита корупційною іржею.

Ми перебуваємо в точці стратегічної розвилки нашого цифрового розвитку на найближче майбутнє. Цифрова компонента нарощує свою частку та вагу у пакеті національних можливостей та загроз України. Сьогодні Україна критично залежить від американського софту та заліза. Основу ІТ-систем наших Сил оборони складає фінансування країн НАТО, і левова частка цих грошей повертається до техногігантів: AWS, Microsoft, Google, Palantir. Уряд та країна змушені маневрувати між нестачею коштів та ризиками домінування американських сервісів (не технологій, а саме сервісів). Питання кооперації з ЄС щодо цифрової автономії, на жаль, не входить навіть до першої десятки пріоритетів держави.

Україна має боротися хоча б за часткове виробництво власних кінцевих сервісів. Будувати своє на базі американських технологій – це вже краще, ніж просто споживати готовий продукт, віддаючи всю додану вартість і потрапляючи у повну залежність. Ми маємо створювати власні «цифрові заводи», щоб забезпечити контроль над даними всередині країни.

Якщо Україна та ЄС рухатимуться далі у обраних напрямках, то через кілька років сторони все гірше розумітимуть одна одну. Несумісність технологічних стеків та законодавства зробить нас чужими. Це і є момент роздоріжжя: як знайти баланс між США та Європою? На жаль, у національній стратегії WinWin-2030 відповідей немає.

Цифрові технології перестали бути просто бізнесом. ШІ (і не лише) робить їх важливою частиною геополітики.

Максим АГЄЄВ,
CEO De Novo

Без чітко окресленої декларації намірів та публічно заявленої стратегії в сфері цифрового суверенітету Україна тупцюватиме на місці. Якщо ми обираємо шлях разом зі США – платимо за їхні сервіси та забуваємо про ілюзії щодо власної унікальності. Якщо прагнемо в Європу – маємо синхронізувати політику з рухом ЄС.

Інвестиційні гроші в країні є, як і готовність їх вкладати, але немає бази для діалогу з урядом. DSUA вже запропонувала концепцію Національної стійкої системи обробки даних. Ми готові діяти, але чекаємо бодай на «рух бровою» з боку держави. Сьогодні я не маю особливого ентузіазму щодо нашого майбутнього. Дуже хочеться помилитися.

Чотири пріоритети на 2026–2027 рр.: що і чому зараз

Аналітика без рекомендацій — це дзеркало без рамки. Красива поверхня, але незручно вішати.

Нижче — не урядова програма і не план для профільного комітету. Це редакційне бачення чотирьох пріоритетів, кожен з яких вирішується дією, а не часом. Якщо доведеться вибирати черговість — Пріоритет 1 є умовою для всіх інших: без захищених людей немає кому будувати архітектуру. Зовнішня умова для всіх чотирьох — участь України в Єдиному цифровому ринку ЄС. Без неї пріоритети є необхідними, але не достатніми.

Пріоритет 1. Закон про цифрове бронювання

Нормативна база є: стаття 17¹ Закону «Про мобілізаційну підготовку та мобілізацію», постанова КМУ № 76/2023. Але нормативна база і система — різні речі. Нормативна база дає право. Система забезпечує результат.

Серед захищених — переважно розробники великих аутсорс-компаній, тоді як Cloud-архітектори держплатформ, DevSecOps оператора критичної інфраструктури, мережеві інженери датацентру — поза реєстром. Не тому, що вони менш важливі. Просто закон ще не визначив критерій «критичності» за функцією.

Ізраїльська модель «кіберрезерву» — не пільга. Це логіка: без цих людей критична система після першого ж удару стає купою металу.

Можливі дії: *визначити реєстр ключових цифрових посад за функціональним критерієм, а не за назвою компанії. Прийняти закон. Провести аудит вже заброньованих ІТ-фахівців на відповідність новим вимогам Постанови № 692 — до дедлайну 1 вересня 2026 р. Запустити постійний реєстр до кінця 2026 року, щоб наступний перегляд критеріїв не застав галузь зненацька.*

Пріоритет 2. Переговорна рамка з гіперскейлерами і позиція українського ринку

Колись ідея зовнішнього якоря здавалася логічною. Тепер ринок говорить інакше. Українська хмара має ставати не майданчиком для чужої експансії, а самостійним вузлом європейської цифрової екосистеми — із власними правилами, юрисдикцією, довірою та здатністю приймати міграцію з глобальних платформ.

Питання для України сьогодні не в тому, чи потрібен гіперскейлер. Воно в тому, на яких умовах глобальний гравець може стати елементом української архітектури, а не її заміною. Польський досвід тут корисний, але не може бути копією: Україна входить у цю розмову з війною, обмеженим капіталом і вже сформованим локальним хмарним ринком.

Тому перший крок держави — не «запросити якоря», а сформувати переговорну рамку. Вона має зафіксувати, які дані і сервіси залишаються під українською юрисдикцією. Які вимоги до телеком-стійкості та енергетичного резервування є обов'язковими. І як не допустити витіснення локальних операторів із ринку.

Українські хмарні оператори і DSUA в цій моделі не є додатком до глобального ринку. Вони є носіями локальної довіри, практики роботи з критичною інфраструктурою і здатності діяти в умовах війни. Саме тому DSUA говорить не про ізоляцію, а про суверенну сумісність: збереження

критичних даних в Україні, міграцію між платформами без штучних бар'єрів і правила, які роблять ринок не слабшим, а більш зрілим.

Польща справді стала хмарним хабом регіону. Але це не шлях для наслідування — це орієнтир: хаб формується там, де є правова рамка, довіра і партнерська, а не залежна інтеграція з глобальними гравцями. Саме цього бракує Україні сьогодні.

Можливі дії: *сформувати переговорну рамку з гіперскейлерами як частину державної цифрової політики. У ній мають бути зафіксовані: роль українських хмарних операторів, умови юрисдикції даних, вимоги до стійкості інфраструктури, сумісність із EUCS і принцип недопущення витіснення локального ринку.*

Пріоритет 3. EUCS-сертифікація — старт у 2026-му, результат у 2027-му

EUCS змінює не лише підхід до сертифікації, а й саме уявлення про зрілість cloud-провайдера. Для України це вже не просто технічний момент, а питання довіри, доступу до капіталу, прогнозованості ринку та здатності працювати за європейськими правилами.

У цьому контексті De Novo і GigaCloud можуть стати першими українськими прикладами того, що національна хмарна індустрія здатна відповідати вимогам ЄС, зберігаючи при цьому власну інженерну автономію.

Польський досвід тут важливий не як модель для копіювання, а як орієнтир: регіональні хмарні рішення розвиваються там, де є передбачуване регулювання, зрозуміла юридична рамка і готовність бізнесу та держави працювати на довгу дистанцію.

Тому запуск процесу EUCS-сертифікації у 2026 році може стати для українських провайдерів не формальністю, а стратегічним входом у новий рівень ринку. Почати у 2026-му — означає відкрити двері для повноцінного результату у 2027-му. EUCS-сертифікація також є ключем до участі в EuroStack Data Spaces — просторах даних, де українські оператори зможуть стати не «зовнішніми постачальниками» для ЄС, а рівноправними учасниками ринку.

Вже з'являються проєкти, де хмара, датацентр і штучний інтелект розглядаються як один інфраструктурний комплекс, а не окремі продукти. Саме в цьому напрямі формується нова логіка відбудови: не просто відновити втрачене, а зібрати технологічну основу для наступного циклу розвитку.

Безпека в цій історії вже не зводиться до кіберзахисту. У 2026 році йдеться про довіру до інфраструктури, прозорість юрисдикції, контроль над даними та здатність провайдера працювати в умовах війни й регуляторного тиску. Саме тому тема суверенної хмари в Україні набуває не модного, а прикладного змісту.

ШІ вже став частиною інфраструктури, а не лише інструментом. У випадку України це означає власну обчислювальну базу, захищені дані та sovereign AI як елемент цифрового суверенітету. Diia AI LLM, AI Factory, Стратегія ШІ до 2030 — це не окремі проєкти. Це частини одного контуру: держава та ринок спільно будують обчислювальну незалежність. Без неї решта архітектури залишається залежною від чужих моделей, чужих чипів і чужих правил доступу до даних.

Можливі дії: *запустити EUCS-підготовку для нацоператорів у 2026-му, а 2027-й зробити роком сертифікаційного результату і публічного доказу зрілості.*

Пріоритет 4. Закон про цифрове посольство — правова рамка

Хмарна евакуація реєстрів у 2022-му — блискуча імпровізація. Але імпровізація — не архітектура. Вона залежить від корпоративної політики AWS або рішення американського Конгресу.

Естонський Data Embassies Act дає зовсім інше: юридично визначений статус резервних копій критичних реєстрів за кордоном з екстериторіальною юрисдикцією — естонське право поширюється на ці дані незалежно від їхнього фізичного місцезнаходження. Постійна синхронізація. Незалежність від воєнної кон'юнктури.

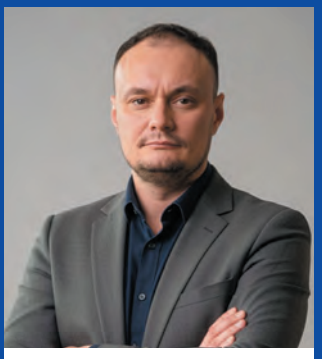
EUCS — ЦЕ ЕВОЛЮЦІЯ ДОВІРИ, А НЕ ПРОСТО СЕРТИФІКАТ

Кирило НАУМЕНКО,
CTO GigaCloud

Я б не називав EUCS повною зміною бізнес-моделі, але це точно значно більше, ніж просто впровадження нових процесів або отримання ще одного сертифіката. По суті, EUCS підіймає вимоги до зрілості cloud-провайдера на всіх рівнях: governance, управління доступами, supply chain, auditability, кібербезпека, контроль над даними та прозорість операційної моделі. Тобто мова йде не лише про технічний compliance, а про формування моделі trusted cloud provider. Для клієнтів це також змінює сам підхід до вибору провайдера. Якщо раніше cloud часто оцінювався через ціну або набір сервісів, то зараз дедалі важливішими стають питання цифрового суверенітету, юрисдикції даних, контролю над інфраструктурою та довіри до оператора. Тому я б сказав, що EUCS – це еволюція операційної моделі cloud-бізнесу в бік більшої прозорості, контрольованості та довіри.

Якщо говорити саме про нерегуляторні фактори, то головна перешкода сьогодні – фінансова. Український ринок має достатньо сильну технічну експертизу для побудови сучасної cloud-інфраструктури. Так само в Україні історично сильна інженерна школа та великий досвід роботи зі складними enterprise– і telecom-рішеннями. Основний виклик – це доступність і вартість капіталу для довгострокових інфраструктурних інвестицій. Побудова sovereign cloud або інфраструктури рівня EUCS потребує дуже великих вкладень у датацентри, резервування, кібербезпеку, compliance, сертифікацію та операційну стійкість. При цьому українські оператори працюють у значно дорожчому фінансовому середовищі, ніж глобальні hyperscaler'и або навіть європейські провайдери. Саме тому питання доступу до інвестицій і прогнозованості ринку сьогодні є ключовими.

vCISO, КОМПЛАЄНС, MISP, MSSP



Сергій БОБРОВ,
технічний директор,
«ЕС ЕН ТІ УКРАЇНА»

Якщо дивитися на кіберзахист не з рівня великої державної архітектури, а з боку конкретної компанії, то головне питання сьогодні – не лише у наявності рішень, а й у їхній керованості. Саме тому в 2026 році зростає роль vCISO, комплаєнсу, MSSP-моделі та систем обміну даними про загрози.

MISP і подібні платформи дають змогу швидше бачити атакувальну картину, але їхній ефект виникає лише тоді, коли бізнес і держава реально обмінюються інформацією. Для середнього і малого бізнесу MSSP стає способом підняти кіберзрілість без надмірного навантаження на власну команду. А для всієї системи критично важливим лишається не лише набір технічних засобів, а підготовлені люди, навчання користувачів і дисципліна у виконанні базових правил. Тобто кібербезпека – це вже не тільки техніка, а й операційна модель, де комплаєнс, аналітика, навчання і відповідальність працюють разом.

Для України вибору немає. Якщо найгірший сценарій реалізується, «держава як платформа» має працювати без фізичної прив'язки до конкретної будівлі. Концепцію «цифрового посольства», яка обговорюється у профільних колах і частково опрацьована у відомчих документах, стримує відсутність політичного мандату у ВРУ. Це не технічна, а вольова перешкода.

Можливі дії: *розробити і прийняти Концепцію «цифрового посольства України» у 2026 році. Переговори з країною-партнером (Люксембург, Нідерланди, Естонія) — паралельно.*

Чотири пріоритети описані мовою рішень держави та великих операторів. Але цифрова архітектура майбутнього не закінчується на рівні урядових стратегій, датацентрів чи національних cloud-провайдерів. Вона неминуче спускається на рівень кожної компанії, яка працює з даними, критичними сервісами, державними замовниками або європейськими партнерами.

Саме тому в цій дискусії з'являється запитання для кожного CTO і CISO приватної компанії: чи сумісна ваша хмарна стратегія з EUCS-вимогами, якщо ваш ключовий клієнт або партнер завтра опиниться у держзакупівлях ЄС? Якщо ні — 2026-й є правильним роком для перегляду не лише інфраструктури, а й усієї моделі кіберуправління.

Висновок. Архітектура — це вибір

У 2022 році один із провідних IT-аналітиків Естонії, дізнавшись про хмарну евакуацію українських державних реєстрів, написав: «Ми тренувалися для цього 15 років. Вони зробили це за 72 години». Ця фраза залишилася в пам'яті не через ефектність, а через точність.

Вона не про те, що Україна виявилася кращою за Естонію. Вона про інше: необхідність іноді стає жорсткішим учителем, ніж стратегія. Але після уроку приходить момент вибору: чи залишиться те, що зроблено під тиском, одноразовою імпровізацією — чи стане архітектурою?

Українська відбудова в цифровій частині вже не може бути лише про закупівлю обладнання чи перенесення сервісів у хмару. Вона має стати про власну обчислювальну базу, про державні й ринкові контури ШІ, про партнерство з ЄС і про здатність не втратити суб'єктність у найважливіший момент. Саме це і є «відбудувати краще» у 2026 році.

Олег СИДОРЕНКО, **МтБ**

▶ ХРОНІКА

Шість країн, один гаманець і тест, який важить більше за саміт

Поки дипломати обговорюють інтеграцію за круглими столами, інженери перевіряють її в коді. На початку червня у Кишиневі на Moldova Digital Summit команда Мінцифри провела перші практичні випробування Дія Wallet за стандартом eIDAS 2.0 – разом із Францією, Нідерландами, Хорватією, Румунією та Молдовою.

Результат: сумісність підтверджена. Передача документів між пристроями через Bluetooth і NFC – працює. Офлайн, без інтернету, у форматі, який ЄС визнає юридично рівнозначним паперовому.

eIDAS 2.0 – не додаток до «Дії». Це єдиний європейський стандарт цифрової довіри. Банк у Нідерландах, страхова в Хорватії, держзакупівельна платформа у Франції – всі вони працюватимуть з однією верифікованою ідентичністю клієнта. Без повторної ідентифікації в кожній юрисдикції, без паперових копій, без нотаріусів.

Для українського B2B це конкретний наслідок: cross-border KYC, підписання контрактів, онбординг у ЄС – стають дешевшими і швидшими. Не через рік. Через місяці.

Прецедент є. Латвія з січня 2026-го визнає українські е-підписи юридично еквівалентними рукописним – перша країна у світі, яка зробила цей крок. Кишинівський тест – наступний доказ: Україна не

наздоганяє стандарт, а формує його разом з ЄС.

Цифрове посольство, суверенна хмара, EUCS-сертифікація – це архітектура держави. Дія Wallet і eIDAS 2.0 – архітектура людини в тій самій системі. Одне без іншого не працює. Суверенітет або тримається на всіх рівнях – або не тримається зовсім.