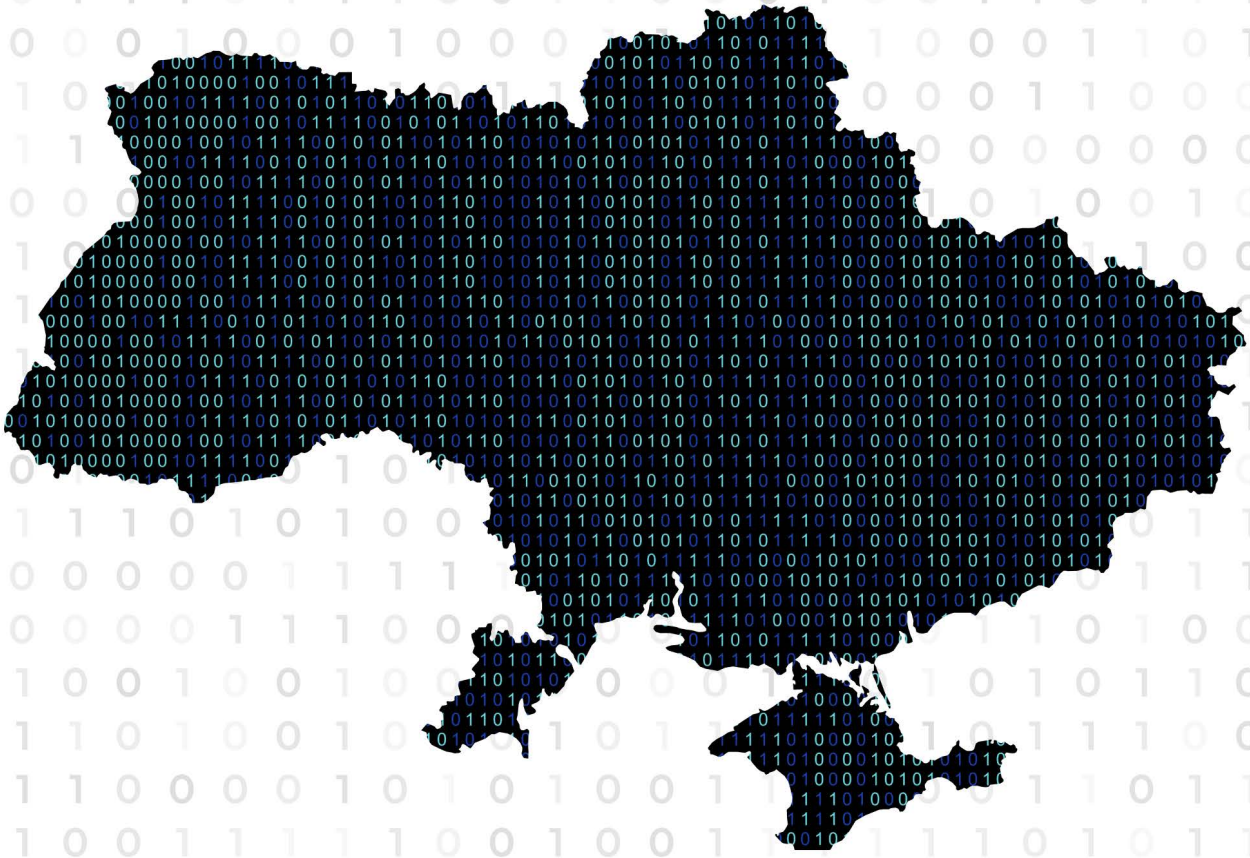
ЦИФРОВИЙ СУВЕРЕНІТЕТ УКРАЇНИ НА ПРАКТИЦІ:

довірена інтеграція як шлях до відновлення, безпеки та глобальної цифрової співпраці



РАДА
ЕКОНОМІЧНОЇ БЕЗПЕКИ
УКРАЇНИ

aws

ЦИФРОВИЙ СУВЕРЕНІТЕТ УКРАЇНИ НА ПРАКТИЦІ:

довірена інтеграція як шлях до відновлення, безпеки та глобальної цифрової співпраці

РЕКОМЕНДАЦІЇ

Це дослідження адресоване насамперед Уряду України та Верховній Раді як суб'єктам ухвалення рішень у сферах цифрового врядування, законодавства про хмарні послуги та інвестицій у відбудову. Воно може слугувати орієнтиром для міжнародних партнерів України — інституцій ЄС, союзників по НАТО, міжнародних фінансових організацій та урядів-донорів, а також для технологічного сектору у взаємодії з рамковою моделлю відбудови України. Дослідження має практичну мету: окреслити політичні рішення, правові реформи та механізми врядування, які б дали Україні змогу безпечно й на українських умовах використовувати вітчизняну, європейську та глобальну цифрову інфраструктуру під час та після відновлення.

Дослідження підготовлено Радою економічної безпеки України у співпраці з Amazon Web Services.

ЦИФРОВИЙ СУВЕРЕНІТЕТ УКРАЇНИ НА ПРАКТИЦІ:

довірена інтеграція як шлях до відновлення, безпеки та глобальної цифрової співпраці

КОРОТКИЙ ЗМІСТ ДОСЛІДЖЕННЯ

КОРОТКИЙ ЗМІСТ ДОСЛІДЖЕННЯ

Планувати регуляторну політику у розпал екзистенційної війни — безпрецедентне завдання у новітній історії. Багаторічне протистояння більшому агресору — один із найвидатніших виявів національного спротиву в європейській історії — боротьба, що дала Україні беззаперечне моральне право самостійно визначати власне майбутнє, зокрема й у цифровій сфері. Водночас це майбутнє забезпечується надвеликою мережею фінансових, військових, технологічних та інституційних міжнародних партнерств. Прагнення розбудувати по-справжньому суверенні цифрові інституції не лише легітимне, а й необхідне. Питання, на яке відповідає це дослідження, — як реалізувати це прагнення так, щоб зміцнити міжнародні партнерства й закласти підвалини успішної відбудови.

Цифровий суверенітет можна визначити як здатність використовувати вітчизняні, європейські та глобальні цифрові спроможності, зберігаючи юридично забезпечений контроль над місцем зберігання даних, доступом до них, ключами шифрування, вимогами безпеки, рішеннями щодо закупівель, стійкістю, переносимістю, можливістю виходу та юридичною відповідальністю. Визначальною є не ізоляція чи місце розташування серверів, а здатність робити усвідомлений вибір. Шлях до цифрового суверенітету пролягає через суворі технічні запобіжники та операційний контроль. Безпека і відкритість не взаємовиключні. За наявності прозорих правил, що враховують можливі ризики, відкритість до довірених технологій зміцнює суверенітет.

Інфраструктура хмарних послуг і даних лежить в основі інфраструктури відбудови. Без неї практично неможливо реалізувати програми відновлення, забезпечити соціальні виплати, публічне адміністрування, закупівлі та безперебійну роботу приватного сектору. Публічна хмара, платформи кібербезпеки, програмне забезпечення світового рівня, інструменти на основі ШІ, дата-центри, телекомунікаційні мережі та системи безперервності послуг так само важливі для відновлення України, як і фізична відбудова доріг, енергомереж та житла, і так само потребують продуманого врядування з першого дня відбудови. Вони також необхідні для підтримки нинішнього темпу цифрових інновацій в Україні та довгострокового повоєнного економічного зростання. Довірена інтеграція — це модель, за якою Україна регулює доступ до вітчизняних, європейських і глобальних цифрових спроможностей відповідно до українського законодавства, узгодженого з визнаними міжнародними та європейськими стандартами. Це модель регульованої взаємозалежності. За Україною зберігаються повноваження щодо класифікації даних, доступу, шифрування, закупівель, стійкості, переносимості, прав на вихід та юридичної відповідальності, а також доступ до довірених технологій, конкурентних ринків і міжнародних стандартів, які підтримують інтероперабельність та інвестиції. Щоб закласти політичну й нормативно-правову основу таких прагнень, Рада економічної безпеки України (РЕБ) пропонує наведені нижче рекомендації:

1. Визнати довірену інтеграцію основою державної політики цифрової відбудови України; визначити цифровий суверенітет як здатність регулювати цифрову взаємозалежність відповідно до українського законодавства і власних політичних рішень, узгоджених із визнаними міжнародними та європейськими стандартами. Тобто встановити чіткі вимоги до класифікації даних, доступу, шифрування, закупівель, стійкості, переносимості, підзвітності та підтвердження надійності провайдерів, а не замінювати міжнародні стандарти суто внутрішніми альтернативами. Не вимагати від України відтворювати чи локалізувати всі глобальні цифрові спроможності всередині держави.
2. Запровадити єдину ризик-орієнтовану систему класифікації даних і робочих навантажень з прив’язкою до хмарних ресурсів, розміщення хостингу, правил

резидентності, закупівель, шифрування та управління ключами, підтвердження надійності провайдерів, переносимості, виходу, резервного копіювання і вимог до відновлення. Така система повинна бути практичною і враховувати параметри конфіденційності, цілісності і доступності без завищення рівня класифікації, що збільшує витрати, сповільнює відновлення або заганяє рутинні робочі навантаження в дефіцитні середовища з високим рівнем захисту.

3. Ухвалити сталі норми, що діятимуть після завершення воєнного стану, щодо використання довірених хмарних послуг, транскордонного резервного копіювання, незасекречених робочих навантажень державного сектору та регульованих секторів, щоб домовленості, досягнуті на основі дозволів, виданих у надзвичайній ситуації, мали міцну правову основу після завершення воєнного стану.

4. Модернізувати законодавче регулювання закупівель хмарних послуг, типові договори, механізми авторизованого перепродажу, критерії підтвердження надійності провайдерів та визнання стандартів, взявши за основу наявну постанову КМУ № 154 (зі змінами, внесеними постановою № 1691 у грудні 2025 року).

5. Вважати відкритий, конкурентний, добре врегульований цифровий ринок інструментом суверенітету, адже завдяки конкуренції зменшується прив’язаність до конкретного постачальника, розширюється вибір і знижується вартість закупівель. При цьому публічний сектор (зокрема центральні і місцеві органи влади, держпідприємства, державні органи та інші державні замовники цифрових послуг) і МСБ отримують доступ до хмарних, ШІ-, кібербезпекових та девелоперських інструментів, які було б занадто дорого створювати на місцях.

6. Забезпечити прозорі та нейтральні щодо постачальників правила закупівель цифрових послуг у публічному секторі. В основі таких правил повинні бути показники безпеки, стійкості, інтероперабельності, переносимості та юридичної відповідальності, з послідовним застосуванням і документуванням ризик-орієнтованих оцінок. Застосовувати обмеження за походженням лише в окремих випадках, коли існують обґрунтовані та документально підтверджені ризики для безпеки.

7. Запровадити обов'язкові паспорти безперервності критичних цифрових послуг із зазначенням інституційного власника, карти залежностей, цільових показників RTO/RPO (цільовий час відновлення та цільова точка відновлення — відповідно, максимально допустимий простій і вікно втрати даних), архітектури резервного копіювання, перевірених механізмів аварійного перемикання, даних про перевірку ризиків постачальників і відповідальних осіб. При цьому базові вимоги до кібербезпеки, стійкості, оцінки ризиків постачальників і зобов'язань щодо прав на вихід повинні бути стандартними передумовами всіх істотних для цифрової сфери інвестицій у відбудову від самого початку, а не додаватися заднім числом після ухвалення архітектурних рішень.

8. Інвестувати у внутрішні цифрові спроможності через українські, європейські та глобальні партнерства: стійкий зв'язок, дата-центри там, де це доцільно, хмарні академії, навчання CISO (керівників з інформаційної безпеки) та CDTO (заступників керівників із цифрової трансформації), впровадження хмарних технологій у МСБ, засоби управління даними, локальних інтеграторів і GovTech-стартапи за підтримки добровільних програм передачі знань, сертифікації, партнерств з університетами, розвитку локальних інтеграторів і механізмів участі МСБ, які нарощують внутрішні потужності, не створюючи нових бар'єрів для закупівель.

Покоління, що займатиметься відновленням України, потребуватиме сучасних і безпечних технологій, які б могли конкурувати на міжнародному рівні. Адже це

означає кращу якість державних послуг, кращі системи освіти й охорони здоров'я, стійкішу фінансову інфраструктуру та нові цифрові продукти для світових ринків. Цифровий суверенітет повинен надати цьому поколінню змогу безпечно користуватися технологіями за українським законодавством, узгодженим із визнаними міжнародними та європейськими стандартами, а не позбавляти доступу до них. Довірена інтеграція перетворює цифрову взаємозалежність із вразливості на управлінський актив: швидша відбудова на безпечній інфраструктурі, вимірювана стійкість, закладена в кожну критичну послугу, можливість управління даними — якість, інтероперабельність, відкриті дані та безпечна аналітика, що розбудовується разом із управлінням хмарними послугами, а не відкладається на пізніші етапи; узгодженість з ЄС, вбудована в закупівлі, а не доточена постфактум, внутрішня цифрова спроможність через контракти й партнерства, а не захищена бар'єрами, які зрештою її послаблюють.

ЦИФРОВИЙ СУВЕРЕНІТЕТ УКРАЇНИ НА ПРАКТИЦІ:

довірена інтеграція як шлях до відновлення, безпеки та глобальної цифрової співпраці

РЕКОМЕНДАЦІЇ ЩОДО ПОЛІТИКИ. ПАКЕТ ДОВІРЕНОЇ ЦИФРОВОЇ ВІДБУДОВИ

РЕКОМЕНДАЦІЇ ЩОДО ПОЛІТИКИ. ПАКЕТ ДОВІРЕНОЇ ЦИФРОВОЇ ВІДБУДОВИ

Матриця рекомендацій містить п'ять груп: базові рішення, які відкривають шлях усьому іншому; інфраструктура і доступ; договори, закупівлі та правова реформа; стійкість і безперервність; спроможність, розвиток ринку й міжнародна співпраця. Рекомендації з першої групи — це передумови для решти; рекомендації наступних груп можна реалізовувати паралельно, як тільки будуть ухвалені фундаментальні рішення.

Група 1 — фундаментальні рішення

Ці три рекомендації — передумови. Без них неможливо послідовно ухвалювати чи контролювати рішення про хостинг, закупівлі, договори, стійкість та партнерства.

Сфера	Рекомендація	Очікуваний результат	Можливий лідер чи партнер
Стратегічне позиціонування	Ухвалити довірену інтеграцію як офіційну основу політики цифрової відбудови України — в законі, урядовій стратегії та міжнародному діалозі, чітко відмежувавши її від суцільної локалізації та некерованої залежності	Зрозумілий політичний курс для парламенту, уряду, міжнародних партнерів, інвесторів та українського технологічного сектору; кінець хибної дилеми «локалізація або хмара»	Верховна Рада, КМУ
Класифікація даних і завдань	Запровадити єдину ризик-орієнтовану класифікацію з трьома-п'ятьма рівнями залежно від потенційних наслідків для конфіденційності, цілісності і доступності. Ілюстративна модель такої системи наведена у третьому розділі. Класифікація повинна бути прямо пов'язана з допустимістю хмари, розміщенням, вимогами до шифрування та управління ключами, стандартами підтвердження надійності провайдерів, показниками RTO/RPO (цільовий час і цільова точка відновлення), зобов'язаннями щодо переносимості та умовами виходу. Уніфікувати термінологію у всіх дотичних законах. Не допускати завищення рівнів секретності	Послідовні й контрольовані рішення про хмару, хостинг, локалізацію, засоби захисту і безперервність для всіх публічних користувачів	Верховна Рада, КМУ, центральний технічний орган, власники державних сервісів
Модель відбудови	Ухвалити модель допустимості хмари на основі класифікації, де кожному рівню відповідають дозволені варіанти інфраструктури: довірена публічна хмара, кваліфікована хмара, гібридна чи суверенна хмара, довірене транскордонне резервне копіювання, контрольовані вітчизняні середовища або спеціалізовані національні або авторизовані з погляду безпеки середовища	Рішення про хостинг, локалізацію, резервне копіювання, стійкість і закупівлі приймаються після оцінки ризику робочого навантаження, а не за універсальними правилами чи політичними уподобаннями	КМУ, МФО, донори, технологічні партнери

Група 2 — інфраструктура і доступ

Ці рекомендації визначають, якою інфраструктурою та на яких умовах користуватиметься Україна. Рішення про внутрішні інвестиції повинні прийматися за класифікаційною моделлю і доказами здійсненності, а не випереджати їх

Сфера	Рекомендація	Очікуваний результат	Можливий лідер чи партнер
Довірена публічна хмара	Зберегти доступ до довірених вітчизняних, європейських і глобальних хмарних провайдерів за українськими нормами, нейтральними до провайдерів, що розроблені з урахуванням технічних запобіжників, параметрів стійкості, інтероперабельності, гарантій безпеки, контролю замовником класифікації і ключів, переносимості та юридичної підзвітності	Швидша й безпечніша модернізація; доступ до найкращих технологій; сильніша кібербезпека; менший тягар фіксованої інфраструктури; ширший простір для інновацій у публічних користувачів	КМУ, довірені надавачі, донори
Вітчизняна інфраструктура[1]	Рішення про вітчизняну хмарну інфраструктуру — дата-центри, регіони чи локальні зони, варто ухвалювати за ринковою логікою, тобто оцінювати вимоги до швидкості відгуку, сигнали попиту, енергетичні й безпекові умови, доступність страхування, готовність кадрів і комерційну життєздатність. Там, де це комерційно виправдано, таку інфраструктуру варто вітати як додану цінність.	Доказові інвестиційні рішення; не витрачати державні кошти на інфраструктуру, що дублює довірені зовнішні ресурси, якщо це не посилює стійкість	КМУ, МФО, інвестори, надавачі хмарних послуг, телекомунікаційні оператори
Транскордонна стійкість і безперервність	Розробити політику довіреного транскордонного резервного копіювання, реплікації та відновлення для окремих функцій забезпечення безперервності: реплікація в реальному чи близькому до реального часі, аварійне перемикання active-active або active-passive там, де це виправдано класифікацією і критичністю сервісу; скрізь, де це відповідає класифікації і юридичним вимогам, вважати розподілене довірене хмарне резервне копіювання в юрисдикціях ЄС пріоритетною моделлю забезпечення безперервності для допустимих робочих навантажень	Захист від фізичного знищення, знеструмлень і ризику регіональної концентрації; відсутність передчасної прив'язки до єдиної моделі забезпечення безперервності	КМУ, партнери по ЄС і НАТО, надавачі хмарних послуг

[1] Рішення про вітчизняну інфраструктуру варто розрізняти за трьома категоріями з різною логікою регулювання і фінансування: (1) комерційно життєздатна інфраструктура, де працюють ринкові принципи і моделі публічно-приватного партнерства; (2) інфраструктура стійкості, що відповідає суспільним інтересам (наприклад, резервні дата-центри, що забезпечують безперервність під час знеструмлень чи атак) і може потребувати державного фінансування у випадках, де комерційної доцільності не достатньо; (3) середовища, що відповідають вимогам безпеки, для секретних завдань — потребують регулювання в логіці національної безпеки та окремого фінансування поза стандартними механізмами закупівель.

Група 3 — договори, закупівлі та правова реформа

Створюють правові й комерційні умови, в яких працює довірена інтеграція. Здебільшого це рішення виконавчої влади й регуляторів. Для першого етапу зміни законодавства не потрібні.

Сфера	Рекомендація	Очікуваний результат	Можливий лідер чи партнер
Закупівлі	Створити сумісні з хмарою механізми закупівель, каталоги послуг і методичні настанови для оцінювання: оплата за споживанням, SaaS, багаторічні договори про надання послуг, критерії вартості життєвого циклу	Швидше, безпечніше й конкурентніше придбання хмарних і цифрових послуг; менше залежності від індивідуальних контрактів	Мінекономіки, Prozorro, Мінцифра
Контракти	Розробити необов'язкові типові положення договорів про надання хмарних послуг у публічному секторі, за моделлю послуг (IaaS, PaaS, SaaS) та рівнем класифікації, з переліком ключових тем: право власності на дані, місце розміщення, зобов'язання щодо безпеки, повідомлення про інциденти (без закріплення конкретних формулювань у законодавстві) із визнанням стандартів BSI C5, ISO/IEC, та звітів SOC.	Менше юридичних непорозумінь; суворіші й послідовніші запобіжники; кращий доступ до ринку і для українських публічних користувачів, і для міжнародних провайдерів, що працюють за українськими нормами	КМУ, правники, постачальники технологій
Переносимість та вихід	Для державних завдань вище рівня «публічний/відкритий» включити до критеріїв закупівель оцінювання механізмів виходу, які пропонує провайдер, можливості експорту даних і документально зафіксовану переносимість сервісів; оприлюднити урядові настанови щодо ключових ризиків і критеріїв оцінювання — планування виходу, строки вивантаження даних, доступність форматів, які замовники повинні зважувати, обираючи провайдера	Менша прив'язка до постачальника; держсектор може мігрувати, відновлюватися чи змінювати постачальника послуг без втрати даних і перерв у роботі	Власники державних послуг, державні замовники, постачальники

Група 4 — стійкість і безперервність

Перетворюють стійкість із гасла на вимірюваний операційний стандарт із чіткою підзвітністю.

Сфера	Рекомендація	Очікуваний результат	Можливий лідер чи партнер
Стійкість критичних сервісів	Запровадити обов'язкові паспорти безперервності для критичних державних цифрових сервісів із зазначенням таких даних: інституційний власник, карта залежностей, показники RTO/RPO, архітектура резервування, випробуване аварійне перемикання, перевірка ризиків постачальників, порядок ескалації. Зробити обов'язковим періодичне тестування і надання публічної звітності в агрегованому вигляді, де детальна технічна архітектура, процедури перемикання і залежності від постачальників лишаються закритими, щоб механізм підзвітності не перетворився на карту цілей для ворога	Підзвітна, перевірена безперервність сервісів; проблеми стійкості видно до того, як вони переростуть у кризові ситуації	КМУ, Держспецзв'язку, CERT-UA, держателі реєстрів
Реконструкція, безпечна за дизайном	Від самого початку, а не в якості модернізації, закласти базові вимоги до кібербезпеки, стійкості, оцінки ризиків постачальників, а також зобов'язання щодо прав на вихід до всіх інвестиційних проєктів з відновлення	Нова інфраструктура не відтворює довоєнних вразливостей; стійкість закладена в проєкт і кошторис, а не вдосконалюється пізніше	КМУ, МФО, донори, власники державних послуг

Група 5 — спроможність, розвиток ринку й міжнародна співпраця

Покликані зміцнити вітчизняну цифрову економіку та інституційну спроможність і забезпечити стійкість довіреної інтеграції після завершення відбудови. Частина пакета — хмарні академії, навчання CISO, кіберполігони, підтримка цифровізації МСБ, розробка паспортів безперервності — підходить для співфінансування МФО і донорами. Впровадження хмарних технологій для малого і середнього бізнесу — питання не лише продуктивності, а й суверенітету. Цифрова економіка, в якій великі компанії користуються передовими хмарними технологіями, ШІ та кіберінструментами, а МСБ бракує навичок, фінансування, сертифікації та доступу до закупівель, стоїть на нерівному фундаменті. Ширше впровадження в МСБ захищених хмарних середовищ, кібергігієни, бухгалтерських, CRM-, e-commerce- та аналітичних інструментів розширює податкову базу, посилює стійкість місцевих ланцюгів постачання і скорочує розрив між експортним IT-сектором та рештою економіки.

Україна може вписати ці рекомендації в програму EU4Digital та механізми Світового банку з фінансування цифрової відбудови й підтримки врядування, збудувавши скоординовану архітектуру фінансування замість фрагментованої попроєктної реалізації.

Сфера	Рекомендація	Очікуваний результат	Можливий лідер чи партнер

Внутрішня цифрова спроможність	Оцінювати інвестиції у фізичну інфраструктуру разом з інвестиціями в людей: стійкий зв'язок, хмарні академії, університетські партнерства, кіберполігони, підготовка CISO і CDTO, команди з управління даними, спроможність локальних інтеграторів. У значних міжнародних технологічних партнерствах заохочувати механізми передачі навичок, сертифікаційні траєкторії, університетські партнерства і розвиток локальних інтеграторів	Створення цінності на місцях, передача навичок, поступове зменшення залежності від зовнішніх виконавців	КМУ, Дія.City, університети, приватний сектор
Діджиталізація МСБ	Підтримати впровадження хмари, кіберстійкість і цифрову продуктивність МСБ шляхом встановлення вимог до участі в закупівлях, субсидування сертифікації, надання доступу до хмарних та ШІ-інструментів за українським законодавством	Ширше економічне відновлення; зайнятість і продуктивність поза великим IT-сектором	КМУ, донори, МФО, бізнес-асоціації
Узгодження з ЄС	Привести правові й регуляторні реформи у відповідність до норм ЄС стосовно даних, кібербезпеки, телекомунікацій, закупівель і цифрового врядування; запланувати порядок впровадження за спроможністю і вартістю забезпечення відповідності; під час кожного етапу оцінювати наслідки узгодження для внутрішнього ринку та надавати МСБ рекомендації щодо переходу	Міцніша інституційна довіра європейських партнерів, поступ на шляху до рішення про відповідність; конкурентний доступ до європейських цифрових ринків	КМУ, інституції ЄС, партнери по ENISA
Побудова коаліцій	Створити коаліцію безпечного цифрового відновлення — уряд, партнери з ЄС і НАТО, МФО, донори, міжнародні технологічні компанії та український IT-сектор — для координації впровадження моделі класифікації, реформи закупівель, стандартів стійкості, розвитку внутрішніх спроможностей та фінансування	Скоординоване впровадження; узгоджений діалог про фінансування та інвестиції; спільна відповідальність за виконання основних етапів	КМУ, партнери з ЄС і НАТО, МФО, донори, технологічні компанії, український IT-сектор

ЦИФРОВИЙ СУВЕРЕНІТЕТ УКРАЇНИ НА ПРАКТИЦІ:

довірена інтеграція як шлях до відновлення, безпеки та глобальної цифрової співпраці

ПОСЛІДОВНІСТЬ ВПРОВАДЖЕННЯ

ПОСЛІДОВНІСТЬ ВПРОВАДЖЕННЯ

Шість наведених нижче пріоритетів впорядковано за залежністю. Пріоритети 1-3 — це фундамент. Там створюються правила управління, від яких залежать усі подальші рішення — хостинг, закупівлі, контракти, стандарти стійкості, інвестиції у спроможності. Пріоритети 4-6 можна визначати й готувати паралельно з пріоритетами 1-3, але їхнє повноцінне впровадження потребує готової базової архітектури. Паралельні напрями, описані наприкінці розділу, повинні стартувати в перший рік у будь-якому випадку: розбудова коаліції, підтримка МСБ, регулювання ШІ та галузеві реформи не потребують системи класифікації, а зволікання з ними накопичує координаційні витрати, які з часом лише зростають. Наскрізна мета полягає в тому, щоб уникнути двох сценаріїв провалу: надмірно централізованої інституційної перебудови, яка з'їдає адмінресурс і не дає робочих інструментів, та фрагментованих попроєктних цифрових закупівель, що фіксують зобов'язання ще до появи регулювання.

Строки залежатимуть від законодавчої спроможності та перебігу війни, але орієнтовний горизонт такий: пріоритети 1–2 (система класифікації та реформа закупівель) — перші 12–18 місяців; пріоритет 3 (критерії підтвердження надійності) — 12–24 місяців; пріоритети 4–6 (паспорти безперервності, узгодження захисту персональних даних, інвестиції у спроможності) — паралельно впродовж 24–36 місяців; паралельні напрями — з першого місяця.

Пріоритет 1: ризик-орієнтована класифікація даних і робочих навантажень

Класифікація — найважливіша передумова з усіх. Від рівня, присвоєного кожному масиву даних чи завданню, залежить все інше: допустимість хмари, розміщення хостингу, правила довіреної юрисдикції, шифрування та управління ключами, стандарти підтвердження надійності провайдерів, вимоги до закупівель, показники RTO/RPO, архітектура резервного копіювання, транскордонна реплікація, здійсненність посольства даних, зобов'язання щодо переносимості, умови виходу. Без універсальної системи такі рішення приймаються окремими підрозділами держсектору хаотично, що поступово і непомітно призводить до правової незахищеності, фрагментованих закупівель та прогалин у стійкості.

За робочу основу можна взяти п'ятирівневу модель із розділу 3: публічний/відкритий; офіційний/внутрішній; чутливий офіційний/з обмеженим доступом; критичний/важливий; секретний/цілком таємний та оборонно-розвідувальний, що ґрунтується на ступенях конфіденційності, цілісності та доступності. Успішна система класифікації дозволяє уникнути завищення рівнів секретності, що може призвести до переповнення захищених середовищ, збільшення витрат і закриття доступу до сучасних хмарних та ШІ-інструментів. Також вона допомагає забезпечити узгоджену термінологію в усіх дотичних законах і розробити рекомендації для держсектора щодо класифікації змішаних масивів даних і взаємопов'язаних сервісів. Для чутливих і критичних завдань кожне рішення щодо класифікації має супроводжуватися документально підтвердженою інформацією про ризики: рівень, відповідальні за функціонал та безпеку, модель хостингу й дозволені юрисдикції, підхід до шифрування та управління ключами, докази відповідності провайдера, показники RTO/RPO, резервне копіювання, аварійне перемикання, реплікація, план переносимості й виходу, прийняті залишкові ризики, ПІБ посадової особи, відповідальної за прийняття залишкового ризику. Класифікація без такого документа — це просто гарна етикетка, а не механізм підзвітності.

Щоб зробити модель робочим інструментом, а не декларацією, її варто оприлюднити в машинозчитуваному форматі. Тоді дотримання можна забезпечувати за допомогою інструментів хмарного управління, позначення ресурсів тегами, обмежувачів (guardrails) та автоматизованих перевірок відповідності.

Пріоритет 2: реформа закупівель хмарних послуг і стандартні договірні гарантії

Після погодження принципів класифікації, під них необхідно оновити правила закупівель і механізми оцінювання. Угоди про надання хмарних послуг повинні мати такі основні пункти: розподіл спільної відповідальності за моделлю послуг; право власності на дані й контроль замовника над місцем розміщення; повідомлення про інциденти та зобов'язання за угодою про рівень послуг; прозорість щодо субпідрядників і обробників; вимоги до переносимості; процедури виходу і доступу до даних після припинення договору; прийнятні докази відповідності. Ці питання повинні бути врегульовані відповідно до настанов про укладання договорів, а не за допомогою прописаних у законодавстві формулювань. Для публічної хмари відповідність вимогам кібербезпеки повинна підтверджуватися незалежними аудиторськими звітами та визнаними сертифікаціями — наприклад, ISO 27001 і звіти SOC 2 Type II. Зобов'язання щодо експорту й видалення даних повинні відповідати хмарній моделі самообслуговування: щоб вилучити чи видалити власні дані без участі провайдера, замовник повинен мати інструменти, API та документацію.

Рекомендації щодо укладення угод варто будувати навколо моделі спільної відповідальності конкретного надавача хмарних послуг, яка визначає межу між обов'язками постачальника і замовника за типом послуги. При цьому під час закупівлі кожної окремої послуги замовники повинні документально закріплювати, яка саме сторона відповідає за конкретні зобов'язання щодо безпеки.

Узгодження захисту персональних даних із GDPR і Конвенцією 108+ — паралельний напрям, який варто розпочати вже на цьому етапі, хоча для формального прийняття необхідне схвалення парламенту. Саме сумісні з GDPR правила визначають, які завдання можна переносити в хмарні регіони ЄС і які угоди з провайдерами юридично доступні. Тобто, закупівельні механізми, розроблені без огляду на GDPR, після узгодження, можливо, доведеться переглядати. Тому рекомендації щодо укладення угод та критерії оцінювання за пріоритетом 2 повинні від самого початку містити сумісні з GDPR зобов'язання, а відомства, відповідальні за закупівлі хмарних послуг та законодавство про захист даних, повинні працювати скоординовано з першого дня впровадження.

Пріоритет 3: критерії підтвердження надійності довірених провайдерів

У процесі формування моделі класифікації, Україні знадобиться прозорий, ризик-орієнтований механізм підтвердження надійності провайдерів, які обслуговують визначені категорії завдань у державному секторі. Це повинна бути відкрита кваліфікаційна процедура, а не закритий «білий список». В першу чергу варто перевіряти засоби безпеки, стійкість, юрисдикційну прозорість, прозорість ланцюга постачання і дотримання санкцій, безпечність розробки, розкриття субпідрядників, здатність реагувати на інциденти, походження компонентів, безперервність бізнесу. Механізм не повинен перетворюватися на суцільне відсіювання за походженням, окрім випадків коли цього прямо вимагає українське законодавство або документально підтверджена оцінка безпеки.

Варто прямо прописати ризики технологічного ланцюга постачання. Можливо, Україні варто звірити власний порядок визначення високоризикових постачальників з методологіями держав ЄС і НАТО для закупівель критичної інфраструктури. Зокрема це стосується європейських схем сертифікації кібербезпеки, вимог NIS2 до безпеки ланцюга постачання та двосторонньої оцінки безпеки з партнерами. Активні консультації з партнерами з ЄС і НАТО щодо компонентів, програмного забезпечення і провайдерів, які становлять ризик для критичної інфраструктури, зміцнили б інтеграційну траєкторію України на шляху до ЄС. Цю практику варто інституціалізувати всередині механізму і застосовувати системно, а не залишати на розсуд організацій держсектора у кожному окремому випадку.

У процесі формування моделі класифікації, Україні знадобиться прозорий, ризик-орієнтований механізм підтвердження надійності провайдерів, які обслуговують робочі навантаження у державному секторі. Ця система повинна функціонувати як відкритий кваліфікаційний процес, а не закритий «білий список». Кожен провайдер, що відповідає визначеним критеріям, повинен мати змогу взяти участь.

Кваліфікація провайдерів має спиратися насамперед на міжнародно визнані незалежні атестації та сертифікації — ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, SOC 2 Type II, BSI C5, а не на вітчизняні системи відповідності, що дублюють уже перевірене незалежними аудиторами. Ці сертифікації втілюють найкращі світові практики кібербезпеки: контроль доступу, шифрування, управління вразливостями, реагування на інциденти, безперервність бізнесу, безпечну розробку і підтримуються безперервними циклами незалежного аудиту. Такий підхід зменшує тертя із забезпеченням відповідності, не зводить бар'єрів для входу на ринок і гарантує, що критерії спираються на перевірені, постійно контрольовані заходи безпеки, а не на разові оцінки. При цьому міжнародна сертифікація — основний доказ відповідності, але не автоматичний дозвіл. Для завдань рівня «чутливий офіційний/з обмеженим доступом» і вище замовники зберігають за собою право і обов'язок проводити додаткову ризик-орієнтовану перевірку, коли це зумовлено чутливістю завдання, міркуваннями юрисдикції чи профілем ланцюга постачання. Механізм має чітко визначати, для яких рівнів достатньо самої лише сертифікації, а для яких потрібна сертифікація плюс додаткова перевірка.

Пріоритет 4: паспорти безперервності критичних сервісів і тестування аварійного перемикання

Практичною відправною точкою могло б стати визначення першої черги критичних державних цифрових сервісів, збій яких матиме найбільше наслідків для громадян, роботи уряду, соціальних виплат, державних фінансів, реєстрів, сервісів ідентифікації чи стабільної роботи економіки. У «паспорті безперервності» для кожного такого сервісу варто зазначити: інституційного власника; ключові технічні залежності та залежності від постачальника; показники RTO і RPO; архітектуру резервного копіювання; перевірене аварійне перемикання; графік тестувань; порядок ескалації; фахівців, відповідальних за кожне рішення в ланцюгу відновлення.

Цінність паспортів у тому, що вони можуть виявити. Сервіс, який неможливо відновити після збою, не можна вважати суверенним, незалежно від його місцезнаходження. Наявність паспорта перетворює стійкість із загальної політичної заяви на вимірювані й перевірювані докази: одиницею підзвітності стає карта залежностей, а не лише показник RTO.

Пріоритет 5: узгодження захисту персональних даних і визнання стандартів

Узгодження з регламентом GDPR і Конвенцією 108+ сприятиме міждержавному обміну даними, зусиллям з євроінтеграції, наблизить рішення про відповідність і закладе правову основу для визнання європейських та міжнародних доказів відповідності в державних закупівлях. З огляду на законодавчий цикл — розробку, консультації із зацікавленими сторонами, перевірку на сумісність із чинним законодавством про безпеку, хмарні сервіси, закупівлі та захист інформації, підготовчу роботу варто починати паралельно з пріоритетами 1 і 2, хоча формальне ухвалення природно триватиме довше. П'яте місце у списку не означає меншу нагальність. Реалізація цього пріоритетного завдання залежить від строків ухвалення законодавства, які неможливо скоротити лише рішеннями виконавчої влади. Рання підготовка — це якраз те, що вбереже механізми пріоритетів 2 і 3 від повторного перегляду після узгодження.

Пріоритет 6: інвестиції у внутрішні цифрові спроможності

Інвестиції у вітчизняну цифрову інфраструктуру — дата-центри, хмарні регіони, локальні зони, стійкий зв'язок — повинні ґрунтуватися на даних щодо попиту, енергетичної стійкості, фізичної безпеки, умов страхування, наявності кадрів, комерційної життєздатності. Символічною даниною цифровому суверенітету вони бути не повинні. Вагоміша інвестиція — в людський та інституційний потенціал, без якого довіреною інтеграцією неможливо ані керувати, ані користуватися: хмарні академії, розроблені спільно з університетами; сертифікаційні траєкторії для держслужбовців і малого бізнесу; програми підготовки CISO і CDTO; кіберполігони; підтримка безпечної міграції; розвиток локальних інтеграторів. Модель CISO Campus, що лише формується в Україні, де лідерство у кібербезпеці розглядають як професійну екосистему зі стандартами компетентності, спільним операційним досвідом і спільнотою від державних інституцій до операторів критичної інфраструктури, задає правильний масштаб амбіції. Фізичні активи без цього інституційного шару — це інфраструктура без суверенної експлуатації.

Управління даними варто розглядати як частину суверенної інфраструктури нарівні з управлінням хмарою. Наступний щабель для України з її місцем у групі A GovTech — не збільшення кількості цифрових послуг, а врядування на основі даних і закладення основ для економіки даних. Серед іншого, це визначення чітких правил якості даних, інтероперабельності, прав доступу, відкритих даних, повторного використання нечутливих даних держсектору, захисту приватності та безпечної аналітики. Досвід ЦНАПів тут повчальний. Цифрова трансформація забезпечує тривалу цінність не тоді, коли модернізує серверні системи, а тоді, коли доходить до практичної взаємодії громадянина з державою через фізичні точки доступу, інклюзивні сервіси, стабільне надання послуг на місцях. Управління хмарою та даними варто проєктувати як єдину систему: захищати чутливі дані, відкривати або надавати спільний доступ там, де це законно й корисно, та повторно використовувати нечутливі дані для покращення державних послуг, інновацій у МСБ і продуктивності приватного сектору.

Паралельні напрями: розбудова коаліції, підтримка МСБ, регулювання ШІ та галузеві реформи

Ці чотири напрями повинні стартувати в перший рік як діалог, підготовка й пілотні проєкти. Вони не потребують систем класифікації до запуску, однак повне впровадження повинно бути прив'язане до базової архітектури у процесі її розбудови.

Коаліція безпечного цифрового відновлення — уряд, партнери з ЄС і НАТО, МФО, донори, міжнародні технологічні компанії, українські IT-компанії, телекомунікаційні оператори, інституції з кібербезпеки, виші та громадянське суспільство — повинна координувати свої дії навколо конкретних результатів: системи класифікації, інструментів закупівель хмарних послуг, паспортів безперервності, індикаторів стійкості, критеріїв підтвердження надійності провайдерів, програм розвитку внутрішніх спроможностей. Коаліція, збудована навколо порожніх заяв, не зможе тривати довго.

Цифровізацію МСБ та участь українського IT-сектору варто розпочинати на ранніх етапах. Насамперед не через додаткові обов'язкові договірні вимоги, а через відкриту, прозору, орієнтовану на результат систему закупівель. Регулювання ШІ повинно відбуватися паралельно з регулюванням хмарних послуг за тією самою логікою класифікації сервісів на основі ШІ, з однаковими стандартами закупівель і вимогами до підтвердження відповідності для постачальників послуг штучного інтелекту. Галузеві регуляторні реформи у фінансах, охороні здоров'я, енергетиці, публічному адмініструванні варто починати з аналізу та виявлення місць, де галузеві правила суперечать єдиній системі класифікації чи дублюють її, і запропонувати впорядкування до того, як ці суперечності стануть частиною договорів закупівлі.

Саме така послідовність дозволяє Україні працювати з донорами, технологічними партнерами та вітчизняними компаніями і водночас не дає імплементаційним програмам зафіксувати зобов'язання до появи нормативної бази, на яку вони повинні спиратися.

ВИСНОВКИ

ВИСНОВКИ

Історія цифрової трансформації України — від Дії до стійкого електронного врядування в умовах війни доводить, що доступ до різноманітних міжнародних технологій і партнерств зміцнив, а не послабив здатність країни служити громадянам і захищати власні інтереси. Такі досягнення стали можливими, бо Україна обрала шлях довіреної інтеграції: відкрито працювати з глобальними інноваціями, зберігаючи за собою право регулювання, юридичну відповідальність та операційний контроль.

Це анітрохи не применшує важливість безпеки, стійкості чи державного контролю. Справжній суверенітет вимагає надійної кібербезпеки, прозорого управління даними, сильних місцевих технічних спроможностей та інституційної здатності ухвалювати незалежні рішення в умовах тиску. Саме це і є справжніми мірилами цифрової незалежності, і найкраще їх досягати в конкурентній, різноманітній технологічній екосистемі, що працює за українським законодавством, узгодженим із визнаними міжнародними та європейськими стандартами.

Від того, що саме Україна вважатиме цифровим суверенітетом, залежатиме цифрова траєкторія країни на покоління вперед. Підхід воєнного часу — відкрити українським інституціям доступ до довіреної хмарної інфраструктури глобального масштабу — зміцнив національну стійкість і операційну безперервність. Українські інституції, громадяни та бізнеси вже працюють на хмарних сервісах, розгорнутих за дозволами, виданими в умовах надзвичайного стану. Тепер, коли Україна вибудовує постійну нормативно-правову базу, головне питання полягає в тому, чи будуть ці перевірені домовленості закріплені на тривалих і передбачуваних умовах. Саме така регуляторна визначеність потрібна міжнародним технологічним партнерам та інвесторам, щоб планувати довгострокові зобов'язання перед цифровим майбутнім України і саме вона надаватиме українським компаніям дедалі більшу роль у виконанні.

Жоден зовнішній гравець — уряд, інституція чи технологічний провайдер — не може і не повинен диктувати Україні, як визначати власний цифровий суверенітет. Міжнародна спільнота може лише поважати й підтримувати право України вільно прокладати цей курс. Модель довіреної інтеграції, описана в цьому дослідженні, може стати частиною цих зусиль, запропонувавши практичну архітектуру класифікації, закупівель, стійкості, підтвердження надійності провайдерів, переносимості, прав на вихід і розвитку спроможностей, водночас віддаючи українським інституціям контроль над рішеннями, що важать найбільше: класифікація даних, доступ, шифрування, підзвітність і відновлення, відкриваючи для громадян, компаній і державних сервісів доступ до найкращих технологій на безпечних, законних і підконтрольних українським інституціям умовах.

Хмарні сервіси, рішення з кібербезпеки та можливості ШІ — стратегічні активи відбудови. Покоління, яке відбудовуватиме Україну, створюватиме з їхньою допомогою кращі державні послуги, сильнішу освіту й медицину, стійкішу фінансову інфраструктуру та нові цифрові продукти для світових ринків. Довірена інтеграція — практична форма цього суверенітету. Вона передбачає врегульований доступ до вітчизняних, європейських і глобальних цифрових можливостей відповідно до українського законодавства, узгодженого з визнаними міжнародними та європейськими стандартами. Україна зберігає за собою контроль над класифікацією, доступом, шифруванням, закупівлями, стійкістю, переносимістю, правами на вихід, підтвердженням надійності провайдерів і юридичною відповідальністю. Це і є цифровий суверенітет на практиці — і він досяжний.

ДЖЕРЕЛА

1. RDNA5, World Bank / Government of Ukraine / European Commission / UN, February 2026, Table 1. URL: https://www.undp.org/ukraine/publications/ukraine-fifth-rapid-damage-and-needs-assessment-rdna5-february-2022-december-2025

2. Guidance Implementing the Cloud Security Principles. URL: https://www.gov.uk/government/publications/implementing-the-cloud-security-principles/implementing-the-cloud-security-principles

3. Criteria for Assessing the Information Security of Cloud Services (PiTuKri). URL: https://kyberturvallisuuskeskus.fi/en/publications/criteria-assessing-information-security-cloud-services-pitukri

4. Italy Information Technology National Strategic Hub Cloud Services. URL: https://www.trade.gov/market-intelligence/italy-information-technology-national-strategic-hub-cloud-services

5. Government on Commercial Cloud. URL: https://www.developer.tech.gov.sg/products/categories/infrastructure-and-hosting/gcc/overview

6. Міністерство цифрової трансформації України, «У Дія.City уже понад 4 тисячі резидентів і 148 тисяч IT-фахівців», 26 березня 2026 року. URL: https://thedigital.gov.ua/news/business/u-diiacity-uze-ponad-4-000-rezydentiv-i-148-000-tysiach-it-fakhivtsiv

7. World Bank, GovTech Maturity Index 2025: Tracking Public Sector Digital Transformation Worldwide, Prosperity Insight Series, 2025, Table 1. URL: https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099032625154535455

8. United Kingdom Government-Cloud (G-Cloud). URL: https://learn.microsoft.com/en-us/compliance/regulatory/offering-g-cloud-uk

9. Accredited information security inspection bodies. URL: https://www.kyberturvallisuuskeskus.fi/en/our-services/assessment-accreditation-and-guidance/accredited-information-security-inspection-bodies

10. Cryptography solutions approved by Traficom's NCSA-FI. URL: https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa/cryptography-solutions-approved-traficoms-ncsa-fi

11. Italy’s Cloud Strategy. URL: https://www.acn.gov.it/portale/en/strategia-cloud-italia

12. Compliance in Italy: Navigating the New Cloud Italy Strategy. URL: https://cloudsecurityalliance.org/blog/2023/03/30/compliance-in-italy-navigating-the-new-cloud-italy-strategy/

13. Policy. URL: https://docs.developer.tech.gov.sg/docs?category=Policy

14. Compliance and Certification. URL: https://www.imda.gov.sg/regulations-and-licensing-listing/ict-standards-and-quality-of-service/it-standards-and-frameworks/compliance-and-certification

15. Doubling down on cloud to deliver better government services. URL: https://www.tech.gov.sg/technews/doubling-down-on-cloud-to-deliver-better-government-services/

16. Government Commercial Agency, "G-Cloud 11 goes live with 4,200 suppliers", 2 July 2019. URL: https://www.gca.gov.uk/news/g-cloud-11-goes-live-with-4200-suppliers.

Про ESCU

Рада економічної безпеки України (ESCU) — незалежна організація, заснована у 2021 році в Києві для протидії зовнішнім і внутрішнім загрозам національній безпеці України та її країн-партнерів.

Вебсайт: www.escu.ua

Facebook: www.fb.com/escofukraine

Автор

Д-р Андрій Пазюк, професор європейського та міжнародного права, спеціальний радник Офісу EPLO в Україні, спеціалізується на правовому регулюванні хмарної інфраструктури, суверенітеті даних і цифровій підзвітності публічного сектору.