На шляху до цифрового суверенітету України: роль системних інтеграторів

Україна вимушено накопичила значний досвід виживання IT-інфраструктури під ворожими ударами. Важливою ланкою у забезпеченні стійкості є компанії-інтегратори.

Війна продемонструвала, наскільки безперервність роботи держави, бізнесу та оборони залежить від цифрової інфраструктури. Однак наявність власних даних, цифрових сервісів або обладнання ще не гарантує можливості самостійно ними управляти. Між окремими технологіями та дієвими системами існує важлива ланка — постачальники IT-послуг, зокрема системні інтегратори. Вони поєднують мережі, обчислювальні ресурси, програмне забезпечення, кіберзахист тощо у керовану інфраструктуру.

Цифровий суверенітет — це здатність контролювати критичні цифрові ресурси та рішення щодо їх використання. У запропонованому IDC підході можна розрізнити суверенітет даних (контроль над їх зберіганням, обробкою і доступом), операційний суверенітет (самостійне управління, захист і відновлення систем) та технологічний суверенітет (контроль ключових технологій).

Жодна складова окремо не гарантує незалежності: навіть дані під національною юрисдикцією можуть залишатися залежними від чужих платформ, обладнання або адміністраторів. Але цифровий суверенітет не тотожний повній відмові від іноземних технологій. Скоріше йдеться про здатність держави та організацій управляти залежностями, забезпечувати безперервність роботи й зберігати контроль над критичними системами.

Українська специфіка: цифрова та фізична стійкість в умовах війни

Український досвід захисту цифрової інфраструктури має особливість: кібератаки відбуваються одночасно з фізичними ударами по інфраструктурі. CERT-UA протягом років фіксує російські кібероперації, зокрема за участі Sandworm та інших угруповань, які відбуваються у безпосередньому зв'язку із фізичними нальотами. Атаки на об'єкти енергетики, зв'язку й датацентри показують, що цифрову безпеку неможливо відокремити від фізичної.

Відтак постачальники IT-послуг мають забезпечувати не лише штатну роботу систем, а й їхню здатність витримувати втрату вузлів, перебої електропостачання та зв'язку, а також швидко відновлюватися після інцидентів. Географічне резервування, незалежні канали, захищений віддалений доступ і локальна інженерна підтримка стають практичними елементами цифрового суверенітету. Хто ж його забезпечує?

Учасники цифрової екосистеми

Цифровий суверенітет формується взаємодією різних учасників: постачальників інфраструктурних послуг, операторів зв'язку, розробників ПО, інтеграторів, оборонних екосистем і міжнародних технологічних партнерів. Їхні функції перетинаються; наведена нижче класифікація (**табл. 1**) має аналітичний характер.

Чому потрібні постачальники IT-послуг

Виробник відповідає за власний продукт, держава визначає правила та вимоги, а системний інтегратор забезпечує сумісність компонентів, захист, керованість і працездатність системи загалом. Розрізнені рішення кількох виробників важко адмініструвати й захищати. Інтеграція перетворює їх на цілісну інфраструктуру, яку можна контролювати та відновлювати.

Зауважмо, що національне походження постачальника саме по собі не гарантує суверенітету. Тривала залежність від одного партнера, непрозора архітектура або надмірні привілеї підрядника можуть створювати нові ризики. Критично важливо, щоб замовник зберігав документацію, контроль доступу, можливість заміни компонентів та незалежного управління системою.

Хмарна інфраструктура: між контролем і стійкістю

Після початку повномасштабного вторгнення Україна прискорила перенесення державних даних у хмару, зокрема за кордон. AWS надала пристрої Snowball для міграції великих масивів інформації. До хмар перенесли сотні державних реєстрів, дані сотень організацій і багато петабайтів інформації.

Ці рішення допомогли зберегти сервіси, але водночас вимушено посилили залежність від зовнішніх постачальників. За оцінкою De Novo, український ринок IaaS/PaaS у 2025 році становив

Таблиця 1. Різні типи компаній-постачальників IT-послуг у схемі цифрового суверенітету України

Тип	Приклад	Що забезпечує
Національні хмарні постачальники/ датацентри	De Novo, GigaCloud, «Парковий» та інші	Зберігання й обробку критичних даних
Телеком-послуги	«Київстар», Vodafone, Datagroup та інші	Мережу, обчислення, власний ШІ
Системні інтегратори	«ЕС ЕН ТІ УКРАЇНА», IT-Інтегратор, Intrasystems, Netwave та інші	IT-інфраструктуру мереж та датацентрів
Розробники ПЗ	SoftServe, EPAM, GlobalLogic та інші	Державні сервіси, реєстри, застосунки
Оборонні платформи	Центр інновацій МОУ (DELTA), Brave1	Розвідку, управління силами та засобами в єдиній системі
Іноземні технологічні партнери	AWS, Microsoft, Google, Oracle, SpaceX	Хмарні послуги, захист даних тощо

$150–155 млн, з яких близько 80% припадало на AWS та Azure.

Для розвитку локальної інфраструктури De Novo, GigaCloud і датацентр «Парковий» створили Альянс цифрового суверенітету. Але недавні атаки на учасників Альянсу є найкращим прикладом того, чому досягнення цифрового суверенітету для України є складнішим, ніж для інших країн. Перед Україною стоїть очевидна дилема: локальне розміщення посилює юрисдикційний контроль, але підвищує ризики фізичних атак; закордонні хмари забезпечують географічне резервування, проте створюють зовнішні залежності. Одним із практичних підходів є гібридна архітектура — розподіл навантажень між українськими та міжнародними ресурсами із забезпеченням переносимості даних і сервісів. Конкретна модель має визначатися критичністю систем, вимогами безпеки та допустимими ризиками.

Телекомунікації

Оператори зв'язку забезпечують цифрову зв'язність, від якої залежить робота державних і військових сервісів, бізнесу та критичної інфраструктури. Їх надійна робота є надзвичайно важливою для збереження суверенітету. Показовим прикладом ризиків стала масштабна кібератака на «Київстар» у грудні 2023 року, що спричинила порушення надання послуг мільйонам абонентів. Для суверенітету не менш важливими, ніж сам факт наявності національних мереж, є резервування, захист операторської інфраструктури та здатність швидко відновлювати зв'язок.

Розробники ПО

Приватні розробники створюють, зокрема, державні цифрові продукти: наприклад, Kitsoft брала участь у написанні «Дії», якою користуються понад 20 млн людей. Diia.City — гарний приклад, того, наскільки масштабна ця галузь в Україні: ініціатива об'єднала понад 4 100 компаній на початок 2026 року; у першому кварталі резиденти простору сплатили 13,4 млрд грн податків — на 68% більше, ніж роком раніше (**рис. 1**). Ці показники — найкраща ілюстрація масштабу та потенціалу щодо побудови цифрового суверенітету, однак безпосередній внесок у нього визначається також контролем над кодом, правами на програмні продукти та можливістю незалежної модернізації.

SoftServe, Sigma Software, Intellias та інші мають масштабні інженерні команди й працюють, зокрема, над державними та оборонними завданнями. Збереження в Україні компетенцій із розроблення й супроводу складних систем є важливою передумовою технологічної самостійності.

Системні інтегратори: ключові гаранти цифрового суверенітету

Системні інтегратори посідають особливе місце у цій команді постачальників IT-послуг. Вони поєднують апаратні та програмні засоби в корпоративні й державні інформаційні системи: мережі, датацентри, системи доступу, кіберзахист та інженерну інфраструктуру. Серед учасників ринку — «ЕС ЕН ТІ УКРАЇНА», IT-Інтегратор, Intrasystems, Seeton, Netwave та інші. Їхній внесок має щонайменше п'ять вимірів. По-перше, архітектурна незалежність: використання сумісних рішень і зменшення прив'язки до одного виробника. По-друге, операційна незалежність: локальні команди, здатні адмініструвати й підтримувати системи. По-третє, кібербезпека: моніторинг, управління доступом і реагування на інциденти. По-четверте, стійкість: резервування та відновлення систем після атак. По-п'яте, збереження національних інженерних експертних знань та досвіду. Якщо підсумувати — ефективність роботи всіх вищеназваних типів національних постачальників IT-послуг безпосередньо залежить від ефективності роботи системних інтеграторів. Саме останні створюють основу цифрового суверенітету й забезпечують його збереження — логічне та фізичне.

Практичні механізми такого впливу можна проілюструвати напрямами діяльності української компанії «ЕС ЕН ТІ УКРАЇНА» (**табл. 2**).

Особливе значення мають центри моніторингу безпеки SOC (Security Operations Center), які допомагають виявляти атаки й контролювати доступ. Фундаментальну роль у створенні цифрової незалежності — на рівні окремих установ та держави в цілому — відіграють також хмарні міграції та впровадження комерційних і корпоративних датацентрів.

Серед замовників «ЕС ЕН ТІ УКРАЇНА» — великі державні та приватні банки, оператори зв'язку, енергетичні та логістичні компанії, державні установи



Рис. 1. Податки резидентів Diia.City за I квартал: 8 млрд грн (2025) проти 13,4 млрд грн (2026), +68%.

Таблиця 2. Напрями рішень «ЕС ЕН ТІ УКРАЇНА» та їх роль у цифровому суверенітеті

Напрям	Що входить	Роль для суверенітету
Корпоративні мережі та зв'язок	Корпоративні мережі, центри обробки викликів, уніфіковані комунікації, інфраструктура Microsoft, Google, Oracle	Мережі держустанов і бізнесу
Підтримка операційних процесів (OSS)	Контроль якості сервісу для операторів, Aiops	Стійкість операторів зв'язку та критичної інфраструктури
Датацентри й дані	ЦОД, резервне копіювання, віртуалізація тощо	Зберігання критичних даних у країні
Інформаційна безпека	SOC, SIEM, контроль доступу (PAM, IdM), захист від DDoS, DLP	Захист держустанов і бізнесу від кіберризиків
Операторські рішення	Оптичні мережі, аналіз трафіку, бездротові канали	Магістральна інфраструктура зв'язку
Інженерія датацентрів	Кабельні системи, живлення, керування кліматом, відеоспостереження, захист інформації	Фізична стійкість вузлів

й військові підрозділи. Це чудово демонструє широту сфер, у яких інтеграція технологій впливає на стійкість критичних систем.

Проте треба враховувати, що інтегратор може стати і джерелом залежності: його компрометація або втрата ключових компетенцій здатні вплинути на багатьох клієнтів.

Оборонні екосистеми

Цікавий та життєво важливий елемент цифрового суверенітету — військові платформи. Вони не просто підвищують обороноздатність. Вони є ключовим елементом захисту суверенітету у найвищому сенсі цього слова, без якого суверенітет цифровий просто втрачає сенс. Саме тому ми вважаємо цифрові військові платформи надважливим елементом, зокрема, цифрового суверенітету, та його невід'ємною частиною — наш досвід останніх років довів це всьому світові.

DELTA — українська військова інтеграційна платформа, що поєднує цифрову мапу, захищений обмін повідомленнями, відео та інструменти планування. Наприклад, на навчаннях НАТО REPMUS 2025 вона продемонструвала координацію понад 100 безпілотних платформ різних типів. Її приклад ілюструє наші можливості операційної інтеграції та контролю над військовими цифровими процесами.

Brave1 об'єднує оборонні стартапи, державу та військових. Інвестиції в українські оборонні технології в цій екосистемі зросли з $5 млн у 2023 році до $105 млн у 2025-му (**рис. 2**). Це показник розвитку національної інноваційної бази, спрямованої на захист суверенітету.



Рис. 2. Інвестиції в український мілтех (екосистема Brave1): $5 млн (2023) → $40 млн (2024) → $105 млн (2025)

Міжнародні технологічні партнери

Міжнародні технологічні компанії відіграли важливу роль у підтриманні стійкості української цифрової інфраструктури. Microsoft допомагала протидіяти кібератакам, Google Project Shield захищав сайти від DDoS-атак (розподілених атак на відмову в обслуговуванні), а Starlink підтримував зв'язок у районах зруйнованих наземних мереж, не кажучи вже про інші моделі використання. Така допомога підвищує стійкість, але водночас створює залежність від приватної іноземної інфраструктури — нещодавно такий приклад, пов'язаний зі Starlink, потрапив у всі світові ЗМІ.

Три ключові перешкоди цифровому суверенітету

Перша — технологічна залежність від іноземних хмар, обладнання, програмних платформ та обчислювальних ресурсів. Її зменшення потребує диверсифікації постачальників, сумісних архітектур і розвитку власних компетенцій.

Друга — недостатня стійкість критичної цифрової інфраструктури до комбінованих фізичних і кібератак. Резервування, розміщення у підземних локаціях, координація реагування та відновлення мають бути частиною проєктування систем, а не лише реакцією на інциденти.

Третя — потреба у зміцненні національних спроможностей управління цифровими системами. Утримання інженерних команд, інвестицій і контрактів в українській юрисдикції, зокрема через Diia.City та подібні ініціативи, сприяють накопиченню технологічних знань.

На щастя, сьогодні у України вже достатньо досвіду, інституцій та міжнародної підтримки: наприклад, через Таллінський механізм — ініціативу координації цивільної кібердопомоги. Практично доведена стійкість нашої цифрової інфраструктури також може стати конкурентною перевагою українських IT-компаній на міжнародних ринках.

Висновки (попередні)

Цифровий суверенітет України не вимагає повної технологічної автономії. Його основою є здатність контролювати критичні цифрові системи, управляти залежностями та забезпечувати їхню безперервну роботу. Держава має визначити стратегічні пріоритети, а технологічний бізнес — допомагати перетворювати їх на практичні спроможності.

Національні постачальники IT-послуг, передусім системні інтегратори, є важливою, операційною ланкою цифрового суверенітету: вони забезпечують сумісність технологій, захист, експлуатацію та відновлення інфраструктури. Їхня стратегічна цінність визначається не лише походженням компанії, а насамперед тим, наскільки її рішення залишають замовникові контроль над архітектурою, даними та доступом.

Український досвід війни вже сформував особливу модель цифрового суверенітету, в якій технологічна незалежність нерозривно пов'язана з фізичною та кібернетичною стійкістю. Сподіваємося, що цей досвід буде враховано нашими європейськими партнерами, але він не знадобиться їм так, як знадобився нам. Варто зауважити, що, з огляду на все сказане, розвиток національних IT-компетенцій, зокрема в галузі системної інтеграції, і партнерство держави з бізнесом слід розглядати не тільки як економічне завдання, а й як складову цифрової безпеки країни.

Олександр САЛИВОН,
консультант з кібербезпеки
SNT Ukraine
+380(44)238–63–88
info@snt.ua, www.snt.ua