Додаток до листа Телекомпалати України від 09.06.2026 р. № 2954

ПОРІВНЯЛЬНА ТАБЛИЦЯ
пропозицій та зауважень до Концепції розвитку хмарних послуг в Україні на період 2026–2031 років

Запропонована редакція	Пропозиції Телекомпалати України	Обґрунтування
Концепція розвитку хмарних послуг в Україні на період 2026–2031 років		
Загальні положення		
Україна прагне стати стійкою, захищеною та інтероперабельною цифровою державою, яка забезпечує безперервність надання публічних (електронних публічних) послуг громадянам та бізнесу в умовах будь-яких кризових ситуацій.		
Ця Концепція розроблена в контексті унікальних та безпрецедентних викликів, пов'язаних із повномасштабною агресією російської федерації. Ці виклики включають постійну загрозу кінетичних ударів по об'єктах критичної інфраструктури (центрах обробки даних), кібератаки та системний дефіцит енергоживлення, що ставить під загрозу безперервність роботи цифрової держави.		
Ця Концепція визначає стратегічні засади розвитку та використання хмарних послуг у публічному секторі та є основою для формування і реалізації державної політики у сфері хмарних послуг.		
Положення цієї Концепції застосовуються суб’єктами публічного сектору, крім випадків, коли особливості використання технологій хмарних обчислень визначаються Національним банком — для банків та осіб, що провадять діяльність на ринках фінансових послуг, та Міноборони — у воєнній сфері та сфері оборони відповідно до Закону України «Про хмарні послуги».		

Ця Концепція спрямована на формування узгодженого підходу до впровадження безпечних, ефективних та інтероперабельних хмарних рішень у державному секторі та визначає цільову модель розвитку хмарної інфраструктури держави, ключові принципи її функціонування, вимоги до кібербезпеки, підходи до закупівель хмарних послуг, а також стандарти сумісності та інтеграції державних інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем (далі – державні інформаційні системи). У публічному секторі України спостерігається поступове зростання використання хмарних послуг як одного з ключових інструментів цифрової трансформації державного управління. Разом із тим рівень впровадження хмарних послуг залишається нерівномірним між різними сегментами публічного сектору, що свідчить про значний потенціал для подальшого масштабування хмарної інфраструктури та послуг.		
Аналіз використання хмарних послуг показує, що основними стримувальними факторами залишаються обмежені фінансові (35%) та кадрові ресурси (31%), високі вимоги до захисту інформації (22%), а також технічна неготовність окремих державних інформаційних систем до переходу у хмарне середовище (22%). Водночас поступове зростання довіри до хмарних технологій та розвиток правового регулювання у сфері хмарних послуг створюють передумови для їх ширшого застосування публічними користувачами.		
На сьогодні у публічному секторі найбільш		

поширеним є використання хмарних послуг за такими видами: 63% організацій використовують програмне забезпечення як послугу, зокрема офісні пакети та системи електронного документообігу; 44% — інфраструктуру як послугу, включно з віртуальними серверами та сховищами даних. Основні робочі навантаження, що розміщуються у хмарі, охоплюють електронний документообіг (52%), публічні веб-портали та сервіси (46%), резервне копіювання та архівування (39%), реєстри та бази даних (35%) та фінансово-облікові системи (29%). Разом із тим потенціал використання більш складних платформних та інноваційних хмарних рішень залишається недостатньо реалізованим, що зумовлює необхідність формування системної державної політики у сфері хмарних послуг.		
Стан розвитку хмарних технологій можна охарактеризувати як перехідний. Більше половини організацій не мають сформованої позиції щодо розширення використання хмарних послуг у середньостроковій перспективі, а майже чверть планують залишити поточний рівень без змін. Разом із тим, прогнозне зростання бюджетних видатків на хмарні сервіси для 2026–2028 років передбачає щорічне збільшення фінансування на 12–15%, що формує значний ринок попиту з боку публічного сектору.		
Для забезпечення сталого та безпечного розвитку хмарних технологій необхідне формування цілісної державної політики у сфері хмарних послуг. Така політика має передбачати розвиток механізмів державного управління сфери хмарних послуг, усунення організаційних		

та фінансових бар'єрів через централізовані закупівлі та прогнозоване фінансування, подолання кадрового дефіциту шляхом підвищення цифрової зрілості (зокрема, підвищення кваліфікації відповідних фахівців), а також формування єдиних принципів вибору, впровадження та використання хмарних рішень.		
Реалізація положень цієї Концепції протягом 2026–2031 років сприятиме підвищенню стійкості та безперервності функціонування цифрової держави України в умовах воєнних, техногенних та кібернетичних загроз. Вона прискорить інноваційну та технологічну трансформацію, що буде досягнута шляхом переходу державних інформаційних систем до моделі використання гібридної хмари із залученням декількох надавачів хмарних послуг (далі — модель гібридної мультихмари). Така модель передбачає поєднання приватних і публічних хмарних середовищ та використання хмарних ресурсів різних надавачів хмарних послуг з метою забезпечення відмовостійкості, масштабованості, технологічної незалежності та диверсифікації розміщення даних. Ключовим елементом такої моделі є суверенний хмарний сегмент, призначений для забезпечення цифрового суверенітету України.		
Опис проблеми, яка потребує розв'язання		
Незважаючи на помітне зростання використання хмарних технологій у публічному секторі, залишаються ключові стримувальні чинники цифрової трансформації. Нерівномірний рівень впровадження хмарних технологій у різних сегментах публічного сектору, зокрема серед центральних, місцевих органів виконавчої влади та органів місцевого		

самоврядування обмежує можливості масштабування сучасних цифрових сервісів.		
Кадрові обмеження також залишаються серйозною перешкодою: нестача кваліфікованих фахівців, здатних забезпечувати управління та інтеграцію хмарних рішень, ускладнює впровадження технологій та підвищує ризики кібербезпеки та затримки трансформації. Високі фінансові витрати на підтримку та міграцію хмарних рішень, зокрема через ефект залежності від одного надавача хмарних послуг та/або послуг центру обробки даних (далі - надавач хмарних послуг), створюють додаткове навантаження на бюджет і підвищують невизначеність у плануванні.		
Технічна застарілість та недостатня готовність інфраструктури обмежують можливості інтеграції хмарних платформ і масштабування автоматизованих процесів, підсилюючи технологічний борг і збільшуючи витрати на підтримку. Водночас високі вимоги захисту інформації та класифікації даних стали обов'язковим критерієм при виборі надавачів хмарних послуг, ускладнюючи міграцію державних інформаційних систем.		
Нерівномірність впровадження хмарних технологій підкреслює потребу в узгоджених підходах та централізованих механізмах підтримки, оскільки державні підприємства та установи адаптують хмарні рішення активніше, ніж центральні, місцеві органи виконавчої влади та органи місцевого самоврядування.		
До всіх зазначених викликів додаються ризики, пов'язані із збройною агресією російської федерації проти України. Вони проявляються у знищенні, пошкодженні або потраплянні		

об’єктів критичної інфраструктури під окупацію, збільшенні частоти кібератак на центри обробки даних та перевантаженні обчислювальних потужностей, а також у тимчасовій недоступності послуг через відключення електропостачання.		
Сукупність цих факторів гальмує масштабування хмарних рішень, обмежує ефективне використання фінансових ресурсів і уповільнює цифрову трансформацію. Вони підкреслюють необхідність розвитку цілісної державної політики, спрямованої на подолання організаційних, фінансових та кадрових бар’єрів, модернізацію ІТ-інфраструктури, підвищення безпеки та забезпечення стійкості державних інформаційних систем навіть в умовах кризових ситуацій.		
Мета і строки реалізації Концепції		
Мета цієї Концепції полягає у забезпеченні стійкості та безперервності функціонування державних інформаційних систем через впровадження національної хмарно-орієнтованої системи, яка гарантує захист державних інформаційних ресурсів від військової агресії, сприяє безперервним інноваціям і модернізації публічних (електронних публічних) послуг, а також дозволяє оперативно реагувати на потреби громадян в умовах воєнного стану та післявоєнного відновлення.		
Ця Концепція розроблена на період 2026–2031 років з урахуванням обмеженості матеріальних ресурсів та безпекових викликів, що виникають через збройну агресію російської федерації проти України.		
Реалізація цієї Концепції передбачає поетапний		

підхід.		
Перший етап (2026–2028 роки) орієнтований на нормативно-правове та інституційне формування:		
- забезпечення нормативно-правового регулювання засад безпечного використання хмарних послуг, зокрема через визначення моделі розподілу відповідальності між публічними користувачами та надавачами хмарних послуг і запровадження класифікації інформації для забезпечення безпеки та відповідності стандартам інформаційної безпеки;		
- створення та запуск моделі Хмарного брокера, Центру компетенцій з хмарних технологій та Центру хмарної безпеки;		
- проведення міграцій державних інформаційних систем у хмарне середовище;		
- розвиток публічно-приватного партнерства у сфері хмарних послуг.		
Другий етап (2029–2031 роки) зосереджений на масштабуванні, інтеграції та оптимізації:		
- перехід публічних користувачів до моделі гібридної мультихмари;		
- інтеграція та взаємодія хмарних ресурсів різних надавачів хмарних послуг для забезпечення безперервності та ефективності;		
- розгортання механізмів резервування та географічного рознесення для підвищення відмовостійкості;		
- оптимізація використання хмарних ресурсів та підвищення рівня автоматизації процесів;		

- підвищення безпеки та стійкості державних інформаційних систем;		
- оцінка результатів реалізації цієї Концепції та, за потреби, коригування подальших заходів її впровадження з урахуванням актуальних потреб цифрового розвитку держави, зокрема пов'язаних із післявоєнним відновленням та європейською інтеграцією України.		
Реалізація цієї Концепції пов'язана з низкою ризиків, серед яких інституційна та організаційна невизначеність, кадровий дефіцит висококваліфікованих ІТ-спеціалістів, обмежені фінансові ресурси та високі витрати на модернізацію і підтримку хмарної інфраструктури. Технологічні ризики включають застарілу інфраструктуру, низький рівень автоматизації та складність інтеграції різнорідних державних інформаційних систем. Особлива увага приділяється безпеці: загроза пошкодження або знищення критичної інфраструктури, відключень електропостачання, кібератак і перевантаження обчислювальних ресурсів може порушити безперервність державних інформаційних систем.		
Основними напрямами державної політики у сфері хмарних послуг, спрямованими на впровадження хмарних послуг, є перехід від фрагментованих локальних ІТ-середовищ до оптимізованої спільної хмарної інфраструктури, забезпечення контролю над критично важливими даними, поєднання внутрішніх ресурсів із масштабованими публічними хмарами, підвищення стійкості та економічної ефективності, узгодження національних		

стандартів із міжнародними та європейськими вимогами, а також створення нових напрямів міжнародного співробітництва. Успішна реалізація цих напрямів сприятиме розвитку хмарних послуг, збільшенню інвестицій та ефективності використання обмежених фінансових ресурсів, а також зміцненню національної цифрової стійкості та цифрового суверенітету.		
Завдання та заходи, спрямовані на розв'язання проблеми		
Розв'язання ідентифікованих проблем у сфері використання хмарних послуг у публічному секторі України потребує системного, поетапного та скоординованого підходу, що поєднує інфраструктурні, організаційні, нормативно-правові, технологічні та кадрові заходи. Реалізація цієї Концепції спрямована на подолання структурної залежності публічних користувачів від застарілих моделей IT-інфраструктури, зниження вразливості державних інформаційних систем до зовнішніх та внутрішніх загроз, а також створення умов для сталого розвитку публічних (електронних публічних) послуг.		
Основними завданнями цієї Концепції є:		
Завдання 1. Забезпечення нормативно-правового регулювання засад безпечного використання хмарних послуг.		
Це Завдання включає формування моделі класифікації інформації за рівнем її критичності, чіткої моделі розподілу відповідальності між надавачами хмарних послуг та публічними користувачами, встановлення підходів до архітектурного проєктування хмарних рішень, а також		

гармонізацію національних стандартів з міжнародними та європейськими стандартами. Це дозволяє подолати інституційну невизначеність і регуляторні бар'єри, що перешкоджають масштабуванню рішень.		
Система класифікації інформації є невід'ємною складовою екосистеми хмарних послуг. Для успішного впровадження хмарних рішень, що відповідають вимогам безпеки та суверенітету, передбачається впровадження моделі класифікації інформації за рівнем її критичності. Така модель базується на оцінці потенційного впливу порушення конфіденційності, цілісності та доступності інформації на діяльність державних органів, національну безпеку, права і свободи громадян та безперервність надання публічних (електронних публічних) послуг.		
Рівень критичності інформації є визначальним фактором для прийняття рішень щодо:		
допустимих середовищ її зберігання та обробки; юрисдикції та географічного розташування; вимог до безпеки та стійкості хмарних рішень.		
Запровадження системи класифікації інформації здійснюється з урахуванням кращих міжнародних практик у сфері хмарних послуг, управління інформаційною безпекою та стійкості цифрової інфраструктури, що застосовуються в державах — членах Європейського Союзу та країнах з розвинутими цифровими екосистемами.		
Для безпечного переходу державних органів до хмарних середовищ, необхідно законодавчо закріпити чітке розмежування відповідальності між публічним користувачем та надавачем		

хмарних послуг — модель розподілу відповідальності.		
Модель розподілу відповідальності повинна чітко розмежовувати обов'язки, де надавач хмарних послуг відповідає за "безпеку хмари", що включає фізичну безпеку інфраструктури, захист обчислювальних ресурсів, мережевих компонентів та середовища функціонування хмарної інфраструктури. Публічний користувач відповідає за "безпеку в хмарі", що охоплює налаштування прикладних систем, управління доступом, обробку та захист власних даних. Така модель спільної відповідальності повинна диференціюватися залежно від виду хмарної послуги (інфраструктура як послуга, платформа як послуга, програмне забезпечення як послуга) відповідно до міжнародних стандартів та практик.		
Без чіткого нормативного розмежування відповідальності між надавачем хмарних послуг та публічним користувачем існує ризик невизначеності щодо виконання вимог кібербезпеки та захисту інформації, зокрема у частині фізичної безпеки інфраструктури та експлуатації хмарного середовища. Закріплення моделі спільної відповідальності сприятиме формуванню зрозумілих правил використання хмарних технологій у державному секторі та створить передумови для безпечної міграції державних інформаційних систем до хмарного середовища.		
Формування безпечної, уніфікованої та стійкої архітектури державних інформаційних систем потребує встановлення єдиних правил і стандартів для створення та розвитку цифрових рішень.		

Ці рішення базуватимуться на таких основних принципах:		
вбудована безпека (проєктування з урахуванням безпеки) — інтеграція заходів кіберзахисту безпосередньо на етапі проєктування інформаційних систем, виходячи з визначеного рівня критичності даних;		
уніфікована структура контролю — використання гармонізованої системи контрольних заходів, що забезпечує комплексне управління ризиками, контроль доступу, проведення аудиту та гарантування безперервності діяльності;		
класифікація інформації — визначення профілю захисту, моделі зберігання та середовища розміщення даних відповідно до ступеня впливу у разі їх порушення;		
взаємосумісність та відкриті стандарти — проєктування рішень із дотриманням принципів сумісності різних систем, уникнення монопольної залежності від одного постачальника послуг та забезпечення підтримки гібридної мультихмарної моделі;		
економічна ефективність — застосування практик фінансового управління хмарними ресурсами для контролю витрат, прозорості бюджетування та переходу від капітальних видатків до операційних (модель оплати за фактично спожиті ресурси).		
Завдання 2. Впровадження моделі Хмарного брокера для закупівлі хмарних послуг.	**Потребує окремого обговорення**	Такий підхід крім позитивних ознак (централізація закупівель, стандартизація, підвищення експертності) несе також суттєві ризики, такі як:

		• надмірна централізація процесу закупівель хмарних послуг; • збільшення строків отримання хмарних сервісів публічними користувачами; • виникнення додаткових адміністративних бар'єрів для міграції державних інформаційних систем у хмарні середовища; • обмеження конкуренції між постачальниками хмарних послуг, що в свою чергу може призвести до штучного здорожчання вартості послуг; • підвищення корупційних ризиків через концентрацію повноважень щодо відбору постачальників та управління закупівлями. В проекті Концепції також відсутні критерії відбору або принципи, на яких буде обиратись (призначатись) Хмарний Брокер, не зазначені його права, обов'язки та відповідальність. На сьогоднішній день діє ПКМУ №154 від 11.02.2025, згідно якої створено реєстр надавачів хмарних послуг. Тому створення додаткового **державного** органу виглядає суперечливо.
Це завдання передбачає централізацію закупівель, прогнозоване фінансування та економічну ефективність використання ресурсів. Модель Хмарного брокера спрямована на подолання фрагментації закупівель хмарних послуг у публічному секторі, зменшення залежності від одного надавача хмарних послуг		

і сприяє впровадженню стандартів інформаційної безпеки та класифікації інформації.		
З метою забезпечення прогнозованості, економічної ефективності та інвестиційної привабливості ринку хмарних послуг держава формує агрегований попит публічного сектору на хмарні ресурси та сервіси. Такий попит визначається на основі централізованого збору планових потреб публічних користувачів, узагальнення інформації щодо обсягів, типів навантажень, рівнів критичності інформації та вимог до безпеки. Агрегований попит використовується для планування закупівель, укладення рамкових та довгострокових договорів, а також як орієнтир для розвитку хмарної інфраструктури та залучення приватних інвестицій.		
З метою централізації закупівель, підвищення економічної ефективності та уникнення фрагментації ринку впроваджується модель Хмарного брокера.		
Хмарний брокер (далі – Брокер) виступає централізованим координатором екосистеми хмарних послуг публічного сектору та забезпечує фінансове і організаційне управління споживанням хмарних ресурсів, включно з прогнозуванням потреб і контролем витрат. Централізація процесів планування та закупівель є необхідною для подолання фрагментації попиту та забезпечення доступу публічних користувачів до економічно вигідних і безпечних хмарних рішень.	**Потребує окремого обговорення**	Пропонуємо передбачити на рівні Концепції визначення: • критеріїв незалежності Хмарного брокера; • порядку його створення або визначення; • вимог до прозорості діяльності; • механізмів контролю за його діяльністю; • процедур оскарження його рішень. Відсутність зазначених положень створює ризики надмірної концентрації повноважень та обмеження конкуренції на ринку хмарних послуг.
Брокер забезпечує виконання таких функцій:		

аналітику та прогнозування шляхом здійснення централізованого збору інформації від публічних користувачів, оцінку їхніх планових потреб у хмарних послугах та прогнозування обсягів споживання на наступні бюджетні періоди для формування ефективної закупівельної політики;		
управління партнерами та каталогом, а саме проводить кваліфікацію надавачів хмарних послуг, адмініструє електронний каталог, створює профілі закупівель та формує конкурентне середовище для отримання найкращих цінових пропозицій;		
відповідає за моніторинг виконання умов контрактів та угод про рівень обслуговування, а також забезпечує юридичні вимоги до портативності даних, що мінімізує ризик монопольної залежності.		
Брокер застосовує диференційовану модель контрактування, відповідно до рівня критичності інформації та значущості державних інформаційних систем:		
для більшості публічних користувачів, у тому числі під час розміщення інформаційних систем об’єктів критичної інформаційної інфраструктури III–IV категорій критичності, Брокер організовує та супроводжує тендерні процедури, за результатами яких договори укладаються безпосередньо між замовниками та надавачами хмарних послуг;		
для розміщення інформаційних систем об’єктів критичної інформаційної інфраструктури I–II категорій критичності Брокер виступає безпосереднім замовником хмарних послуг, укладає довгострокові договори з надавачами		

хмарних послуг, та забезпечує доступ власників систем до таких ресурсів у встановленому порядку.		
Впровадження моделі Брокера сприятиме переходу публічного сектору від капітальних витрат до операційної моделі використання хмарних ресурсів, забезпечить прогнозованість бюджетних видатків та дозволить укладати довгострокові рамкові договори, що знижують цінові ризики та витрати на міграцію між надавачами хмарних послуг.		
Завдання 3. Створення Центру компетенцій з хмарних технологій.		
Центр компетенції з хмарних технологій (далі - Центр компетенцій) покликаний вирішити проблему дефіциту кваліфікованих ІТ-фахівців шляхом організації навчальних програм, надання методичної та консультативної підтримки публічним користувачам у процесі переходу до хмарних технологій, а також супроводу архітектурної модернізації державних інформаційних систем. Центр компетенцій здійснюватиме оцінку доцільності міграції державних інформаційних систем у хмарне середовище та прийматиме рішення щодо обов'язковості такої міграції або щодо її обмеження (відтермінування чи заборони) з урахуванням критеріїв економічної ефективності, вимог інформаційної безпеки, рівня критичності державних інформаційних систем та інших визначених критеріїв. Центр компетенцій сприятиме підвищенню цифрової зрілості публічних користувачів та створенню умов для впровадження і масштабування сумісних, безпечних та інноваційних хмарних рішень, а також забезпечуватиме практичну	**Потребує окремого обговорення**	Вбачаємо той самий набір ризиків, що перечислені вище стосовно впровадження моделі Хмарного брокера для закупівлі хмарних послуг.

реалізацію принципу обґрунтованого та безпечного використання хмарних технологій (Cloud Smart) шляхом формування та застосування єдиних підходів до вибору моделей розміщення державних інформаційних систем.		
Центр компетенцій створюється як ключовий технічний та консультативний орган, що забезпечує експертизу архітектурних рішень, планування міграції, модернізацію державних інформаційних систем, підготовку кадрів та стандартизацію хмарних рішень.		
Центр компетенцій забезпечує:		
проведення експертизи архітектурних рішень державних інформаційних систем з метою оцінки їх готовності до міграції у хмарне середовище та аналізу ефективності використання хмарних ресурсів;		
комплексне планування міграції державних інформаційних систем та інформації у хмарне середовище;		
технічну адаптацію та модернізацію державних інформаційних систем, зокрема модернізацію програмного забезпечення із застосуванням контейнеризації та безсерверних технологій для підвищення їх мобільності та масштабованості;		
розробку та впровадження технологій автоматизованого розгортання інфраструктури для автоматизації та стандартизації розгортання ресурсів;		
розробку та тестування планів відновлення після аварій для гарантування безперервності надання послуг;		
постійну оптимізацію використання обчислювальних ресурсів та підвищення		

ефективності витрат;		
формування та валідацію технічних завдань на розробку або модернізацію державних інформаційних систем відповідно до кращих хмарних практик;		
розробку вимог до архітектури, що забезпечують автономність та стійкість публічних користувачів у хмарному середовищі;		
навчання моделям сучасних хмарних обчислень для подолання кадрового дефіциту у сфері хмарної архітектури, безпеки та управління, забезпечуючи, що фахівці публічних користувачів готові до сучасних хмарно-орієнтованих середовищ;		
керування впровадженням готових рішень та автоматизацією перевірки відповідності. Це сприяє взаємосумісності та зменшує необхідність кожного органу влади розробляти власні унікальні та затратні рішення, які можуть бути несумісними з національною архітектурою.		
Завдання 4. Створення Центру хмарної безпеки.		
Це завдання спрямоване на посилення інформаційної безпеки та відповідності нормативним вимогам. Центр хмарної безпеки здійснюватиме аудит і безперервний моніторинг безпеки, що є критично важливим для захисту державних інформаційних ресурсів від кібератак та інших загроз, включно з наслідками збройної агресії. Крім того, Центр хмарної безпеки виконуватиме функції галузевого центру моніторингу кібербезпеки (SOC) та реагування на комп'ютерні інциденти (CSIRT) у сфері хмарних послуг, забезпечуючи повний цикл виявлення, аналізу та реагування на		

кіберінциденти, координацію заходів з їх ліквідації, а також обмін інформацією про кіберзагрози з уповноваженими суб'єктами національної системи кібербезпеки.		
Центр хмарної безпеки створюється для забезпечення єдиного підходу до управління ризиками, моніторингу та реагування на кіберзагрози, кібератаки та кіберінциденти у хмарному середовищі.		
Центр хмарної безпеки забезпечує:		
здійснення моніторингу параметрів налаштування хмарної інфраструктури для виявлення ризиків та невідповідностей політикам безпеки;		
інтеграцію перевірок та політик безпеки безпосередньо в процеси розробки та розгортання інфраструктури, що дозволяє автоматизувати дотримання вимог;		
створення та супроводження безпечних середовищ розгортання хмарної інфраструктури для різних середовищ, що відповідають вимогам законодавства у сфері кібербезпеки та захисту інформації;		
захист публічних сервісів від веб-загроз та атак типу «відмова в обслуговуванні»;		
централізований збір та аналіз подій безпеки, а також забезпечення першої лінії реагування на виявлені кіберінциденти;		
надання та контроль використання безпечних налаштувань за замовчуванням для середовищ контейнеризації та віртуалізації;		
розробку базових вимог (профілів) безпеки та перевірку відповідності державних інформаційних систем профілю безпеки для розміщення в хмарі.		

Завдання 5. Розвиток публічно-приватного партнерства.		
Це завдання забезпечує інтеграцію внутрішніх (суверенних) ресурсів з гнучкими та масштабованими публічними хмарними платформами, стимулює інвестиції у хмарну інфраструктуру та розвиток інноваційних хмарних послуг. Партнерство дозволяє забезпечити економічну ефективність, розподіл ризиків та оперативну підтримку критично важливих державних інформаційних систем.		
Збройна агресія російської федерації зумовила необхідність підвищення стійкості державної цифрової інфраструктури, зокрема шляхом розміщення центрів обробки даних у локаціях з низькою ймовірністю кінетичного ураження, високим рівнем фізичного захисту та енергонезалежності. Однією з відповідей на ці виклики є створення та модернізація захищених центрів обробки даних, у тому числі підземних та географічно рознесених об’єктів, а також розвиток захищених хмарних середовищ для потреб публічного сектору.		
В умовах обмеженості бюджетних ресурсів держава передбачає залучення приватного сектору до створення, модернізації та експлуатації хмарної інфраструктури шляхом застосування механізмів публічно-приватного партнерства. Публічно-приватне партнерство у сфері хмарних послуг розглядається як інструмент забезпечення масштабованості, економічної доцільності та прискореного розвитку хмарної інфраструктури, а також залучення інвестицій, експертизи та інновацій приватного сектору.		
У межах таких партнерств приватний партнер		

забезпечує фінансування, створення та експлуатацію відповідної інфраструктури, тоді як держава формує прогнозований попит на визначені категорії хмарних і мережевих ресурсів, зокрема для розміщення та резервування державних інформаційних ресурсів і критичних державних інформаційних систем. Такий підхід дозволяє поєднати вимоги національної безпеки та цифрового суверенітету з економічною ефективністю інвестицій.		
Реалізація публічно-приватного партнерства у сфері хмарних послуг здійснюється з дотриманням принципів прозорості, технологічної нейтральності, конкуренції та чіткого розподілу ризиків між сторонами, а також із забезпеченням передбачуваності та стабільності довгострокових договірних зобов'язань у межах чинного законодавства України. Такі партнерства можуть передбачати укладення довгострокових договорів на створення або модернізацію захищених центрів обробки даних, надання хмарних послуг або потужностей, сервісну модель оплати за фактично доступний або зарезервований обсяг ресурсів, а також використання механізмів державного замовлення та міжнародної технічної допомоги.		
Завдання 6. Впровадження моделі гібридної мультихмари та підходів резервування для публічних користувачів.		
Це завдання спрямоване на забезпечення стійкості та безперервності функціонування державних інформаційних систем, з урахуванням ризиків, пов'язаних зі збройною агресією, кібератаками і відключеннями електропостачання. Воно включає		

масштабування використання хмарних рішень для всіх публічних користувачів, інтеграцію національних і публічних хмарних середовищ, впровадження механізмів резервування та географічного рознесення даних для підвищення відмовостійкості.		
Ключовим завданням забезпечення стійкості та безперервності цифрової держави є створення архітектури, яка гарантуватиме безперервність функціонування критичних державних інформаційних систем, навіть в умовах воєнних дій, кібератак або енергетичних криз та спрямована на:		
фізичний захист інфраструктури — будівництво або модернізація укріплених центрів обробки даних, стійких до кінетичних ударів та перебоїв з енергопостачанням;		
диверсифікацію розміщення даних — створення розподілених центрів обробки даних, включаючи резервні майданчики за межами України;		
інтеграцію в міжнародну екосистему безпеки — застосування міжнародно визнаних стандартів та практик управління ризиками, кіберзахисту, безперервності діяльності та захисту інформації.		
Однією з головних причинно-наслідкових проблем, яку вирішує ця Концепція, є напруга між традиційним розумінням суверенітету даних (зберігання даних на території України) та нагальною потребою у стійкості/безперервності (розміщення резервних копій за межами України через ризики війни). Для забезпечення доступності державних інформаційних ресурсів, держава застосовує гнучкий підхід до розміщення та		

резервування інформації, що допускає екстериторіальне розміщення (за умови здатності у прийнятний час відновлюватися на кожній із сторін резервування), як найвищий пріоритет для гарантування життєздатності критичних функцій. Такий підхід є необхідною умовою забезпечення безперервності функціонування державних інформаційних ресурсів, що є головним завданням в умовах воєнного стану.		
Для подолання згаданих викликів національна архітектура хмарної інфраструктури України формується на основі моделі гібридної мультихмари, яка передбачає інтеграцію національної (суверенної) хмари, публічних хмар та мережі Посольств даних. Такий підхід мінімізує ризик відмови та забезпечує географічну відмовостійкість державних інформаційних систем, а також забезпечує прозорість та чесну конкуренцію при виборі надавачів хмарних послуг. Застосування моделі гібридної мультихмари забезпечує баланс між вимогами безпеки, економічною ефективністю, гнучкістю використання обчислювальних ресурсів та розподілом технологічних ризиків, а також сприяє уникненню залежності від одного надавача хмарних послуг. Зазначена модель включає такі основні складові:		
1) національна (суверенна) хмара — це консолідований сегмент інфраструктури приватної хмари, що складається з мережі взаємопов'язаних, високозахищених центрів обробки даних, розташованих виключно на території України з обов'язковим географічним розподілом та є фундаментом для забезпечення фізичної резидентності	національна (суверенна) хмара — це консолідований сегмент інфраструктури приватної хмари, що складається з мережі взаємопов'язаних, високозахищених центрів обробки даних, розташованих на території України, **а також інформаційно-комунікаційних систем (ІКС), що належать резидентам України і**	До суверенної хмари слід також відносити інформаційно-комунікаційні системи (ІКС), що належать резидентам України і розташовані в закордонних ЦОД. Архітектура з використанням закордонних ЦОД для розміщення ІКС для надавачів хмарних послуг, в тому числі публічному сектору, є

даних та безперервної обробки інформації, що становить державну таємницю та критичних даних об’єктів критичної інформаційної інфраструктури, для яких чинне національне законодавство висуває вимогу 100% локалізації; державні інформаційні системи, що вимагають високого рівня контролю, глибокої інтеграції з існуючими IT-системами та використання власних пропрієтарних ліцензій.	**розташовані в закордонних центрах обробки даних,** з обов'язковим географічним розподілом та є фундаментом для забезпечення фізичної резидентності даних та безперервної обробки інформації, що становить державну таємницю та критичних даних об’єктів критичної інформаційної інфраструктури, для яких чинне національне законодавство висуває вимогу 100% локалізації; державні інформаційні системи, що вимагають високого рівня контролю, глибокої інтеграції з існуючими IT-системами та використання власних пропрієтарних ліцензій.	сталою практикою серед українських хмарних провайдерів. Такі ІКС, як правило забезпечують вимоги користувачів, в тому числі публічних, по резервуванню та забезпеченню відновлення у разі критичної ситуації в одному або декількох ЦОД на території України. Тому пропонуємо розширити можливості для розташування хмарних ЦОД надавачів за межі України із забезпеченням національних та міжнародних стандартів інформаційної безпеки. З проєкту документу також не зрозуміло, чи перелік даних для розміщення в національній хмарі є вичерпним, але з огляду на впровадження інституту Хмарного Брокера та Центру компетенцій з хмарних технологій є великі ризики монополізації та звуження конкуренції.
Національна (суверенна) хмара є прямою відповіддю на загрози воєнного часу. Вона забезпечує фізичний суверенітет та стійкість проти кінетичних ударів і дефіциту енергоживлення через розміщення центрів обробки даних у підземних або значно зміцнених спорудах на території України, відповідно до вимог національної безпеки, забезпечення можливості оперативного відновлення після збоїв, коли дані мають залишатися в межах країни та використання моделі повністю ізольованої приватної хмари, що підтверджено успішним розгортанням критичних державних інформаційних систем.		
Національна (суверенна) хмара також забезпечує повний контроль над управлінням		

ключами шифрування, ідентифікацією та доступом, а також функціонуванням критичних державних інформаційних систем, для яких вимоги до конфіденційності, цілісності та доступності є визначальними.		
Національна (суверенна) хмара призначена для розміщення та обробки найбільш чутливої державної інформації, керуючись принципом «суверенітет передусім», зокрема:		
інформації, що становить державну таємницю;		
інформації об'єктів критичної інформаційної інфраструктури;		
інформації, для якої вимоги до конфіденційності, цілісності та доступності є безумовними відповідно до законодавства України;		
інформації, що потребує повного контролю над ключами шифрування та гарантій їх юридичної недоторканності;		
критичних державних інформаційних систем, пов'язаних з управлінням ідентифікацією та доступом, а також управлінням національними криптографічними ключами.		
Національна (суверенна) хмара забезпечує юридичну визначеність та повну незалежність від зовнішніх впливів шляхом:		
юрисдикційного контролю, за якого обробка інформації та доступ до неї регулюються виключно законодавством України, що мінімізує ризики застосування екстериторіальних норм іноземного права;		
забезпечення найвищого рівня конфіденційності як невід'ємної складової цифрового суверенітету держави;		
2) публічна хмара є важливим		

компонентом моделі гібридної мультихмари, що забезпечує можливість використання масштабованих, гнучких та економічно ефективних обчислювальних ресурсів, здатних швидко адаптуватися до зростання навантаження та змін потреб публічних користувачів. Її використання також забезпечує доступ до сучасних інноваційних хмарних платформ і готових прикладних сервісів, що сприяє розвитку цифрових сервісів держави. Окремим елементом такої моделі є використання центрів обробки даних у довірених іноземних юрисдикціях для екстериторіального географічного резервування державних інформаційних ресурсів з метою забезпечення безперервності функціонування критичних державних інформаційних систем у разі пошкодження або втрати внутрішньої інфраструктури;		
3) Посольство даних — це модель екстериторіального розміщення державних інформаційних ресурсів України за межами її території з метою забезпечення їх збереження та безперервності функціонування.		
Посольство даних може реалізовуватись у двох форматах:		
розміщення центру обробки даних на території закордонної дипломатичної установи України іноземної держави – держави партнера України.		
Таке розміщення забезпечує збереження повного суверенітету та юридичної недоторканності критичних державних інформаційних ресурсів та їхніх резервних копій, оскільки, згідно з міжнародним правом, приміщення закордонної дипломатичної установи України вважається суверенною		

територією України;		
розміщення центру обробки даних на території іноземної держави – держави партнера України, із забезпеченням повного контролю України за зберіганням, обробкою та захистом даних та виключного контролю над доступом до них.		
Таке розміщення ґрунтується на механізмі міжнародно-правового захисту, що забезпечує спеціальний режим розміщення та використання відповідної інфраструктури, зокрема шляхом надання орендованим приміщенням та технічним засобам статусу, еквівалентного режиму дипломатичної недоторканності, та визначення застосовного права України до інформації, що в них обробляється. Такий підхід дозволяє розглядати відповідне хмарне середовище як функціональне розширення національної цифрової інфраструктури за межами території України.		
Таким чином, Посольство даних гарантує найвищий рівень фізичної та правової безпеки даних із гарантуванням контролю України за їх зберіганням і обробкою у межах узгодженої з іноземною державою – державою партнером України моделі управління та захисту даних, залишаючись при цьому за межами військової досяжності на території України.		
Ця Концепція передбачає розподіл інфраструктури зберігання та обробки даних на національні та іноземні центри обробки даних, де для інформації високого рівня критичності передбачається її зберігання у національній (суверенній) хмарі України — захищених державних центрах обробки даних, включно з захищеними від кінетичних ударів центрами		

обробки даних, здатними функціонувати в умовах воєнних загроз та обмеженого енергопостачання, а резервне копіювання такої інформації здійснюється в довірених іноземних юрисдикціях у центрах обробки даних, розміщених за межами території України в межах моделі Посольства даних, що відповідають міжнародним стандартам безпеки, з метою забезпечення безперервності функціонування державних інформаційних ресурсів у разі втрати або пошкодження внутрішньої інфраструктури.		
Резервування розглядається як один із ключових елементів стійкості державної хмарної інфраструктури та обов'язкова умова безперервності функціонування державних інформаційних ресурсів.		
Ця Концепція закладає такі базові принципи резервування інформації, що застосовуються залежно від рівня її критичності:		
принцип географічного рознесення — резервні копії зберігаються у різних фізичних локаціях, що мінімізує ризики втрати інформації внаслідок надзвичайних ситуацій;		
принцип юрисдикційного контролю — резервування інформації здійснюється у довірених іноземних юрисдикціях, що забезпечують належний рівень правового захисту даних;		
принцип багаторівневості — використання кількох резервних копій, розміщених у різних середовищах, для забезпечення надійного та швидкого відновлення інформації та цифрових сервісів держави;		
принцип технологічної стійкості — резервування охоплює не лише інформацію, а й		

інфраструктуру та середовище її обробки, що дозволяє суттєво скоротити час відновлення роботи державних інформаційних систем;		
принцип пропорційності — обсяг та складність резервування визначаються відповідно до рівня критичності інформації, потенційних ризиків її втрати та вимог до безперервності функціонування державних інформаційних систем.		
Кожне завдання безпосередньо відповідає ідентифікованим проблемам та ризикам (кадрові та фінансові обмеження, технічна застарілість, інституційна невизначеність, регуляторні та безпекові вимоги, загрози від збройної агресії), і разом формують цілісний підхід до реалізації цієї Концепції на 2026–2031 роки, з поетапним нарощуванням масштабів, інтеграцією та оптимізацією хмарної інфраструктури.		
Очікувані результати та показники їх досягнення		
Реалізація цієї Концепції забезпечить трансформацію України в одну з найбільш стійких та безпечних цифрових держав світу, в якій хмарні технології є гарантом безпеки та ефективності державних інформаційних ресурсів, і дозволить досягти таких результатів:		
забезпечено системний перехід публічного сектору до моделі гібридної мультихмари, з метою гарантування безперервності функціонування державних інформаційних ресурсів у кризових та воєнних умовах;		
створено умови для гарантованої катастрофостійкості критичних державних інформаційних ресурсів, включно з можливістю відновлення їх функціонування у стислі строки		

навіть у разі втрати внутрішніх обчислювальних потужностей;		
запроваджено єдину модель управління споживанням хмарних ресурсів, що передбачає централізоване планування, закупівлю та контроль використання хмарних послуг через механізм Брокера;		
створено інституційну спроможність для прийняття обов'язкових архітектурних рішень у сфері хмарних послуг, зокрема через функціонування Центру компетенцій як суб'єкта оцінки доцільності, безпечності та економічної ефективності міграції державних інформаційних систем;		
забезпечено впровадження принципу обґрунтованого та безпечного використання хмарних технологій (Cloud Smart) у публічному секторі, що унеможливлює необґрунтовані або ризикові міграції, зменшує технологічну залежність від окремих надавачів хмарних послуг та оптимізує використання бюджетних коштів;		
створено галузевий Центр хмарної безпеки, який забезпечує централізований моніторинг, аудит, управління ризиками та реагування на кіберінциденти у хмарному середовищі публічного сектору;		
запроваджено систему класифікації інформації та модель розподілу відповідальності, що створює правову визначеність для безпечного використання хмарних послуг у державних інформаційних системах;		
забезпечено модернізацію та будівництво захищених, енергоефективних і географічно розподілених центрів обробки даних, включно зі стійкими до авіаударів центрами		

обробки даних та екстериторіальними майданчиками резервування;		
забезпечено перехід публічного сектору від капітальних витрат до операційної моделі використання хмарних ресурсів, що дозволить оплачувати лише фактично спожиті обчислювальні потужності, із одночасним скороченням термінів розгортання нових державних інформаційних систем, завдяки використанню готових хмарних платформних рішень;		
створено умови для залучення приватних інвестицій у розвиток хмарної інфраструктури шляхом запровадження інструментів довгострокового планування споживання, цільових податкових пільг та інноваційних фінансових механізмів мінімізації ризиків приватних інвесторів, зокрема із застосуванням механізмів публічно-приватного партнерства та довгострокових договорів;		
забезпечено гармонізацію хмарної інфраструктури України зі стандартами Європейського Союзу, що створює передумови для європейської інтеграції України та безпечного транскордонного обміну даними.		
Одним із основних інструментів реалізації цієї Концепції є плани заходів, що розробляються для кожного з етапів реалізації цієї Концепції та якими передбачаються конкретні заходи, індикатори досягнення цілей та визначається перелік відповідальних органів.		
Обсяг фінансових, матеріально-технічних, людських та інших ресурсів		
Заходи з реалізації цієї Концепції здійснюються протягом 2026 — 2031 років за рахунок та в межах коштів державного і місцевих бюджетів,		

затверджених на відповідний рік, а також за рахунок коштів міжнародної технічної допомоги та міжнародних організацій, інших джерел, не заборонених законодавством України.		
Порядок проведення моніторингу, оцінки результатів реалізації Концепції та звітування		
Забезпечення координації дій з реалізації цієї Концепції, здійснення контролю за її реалізацією, проведення моніторингу, оцінки результатів її реалізації здійснює Мінцифри разом із заінтересованими центральними органами виконавчої влади, підприємствами, установами та організаціями.		
Моніторинг реалізації цієї Концепції проводиться Мінцифри щороку шляхом збору та опрацювання інформації про стан її реалізації.		
За результатами проведення моніторингу передбачається підготовка та подання раз на три роки Кабінетові Міністрів України звіту про стан реалізації цієї Концепції, а також його розміщення на офіційному веб-сайті Мінцифри.		
Оцінювання результатів реалізації цієї Концепції здійснюється Мінцифри за визначеними в планах заходів з реалізації цієї Концепції показниками з урахуванням результатів моніторингу виконання завдань та заходів цієї Концепції, про що зазначається у звіті.		