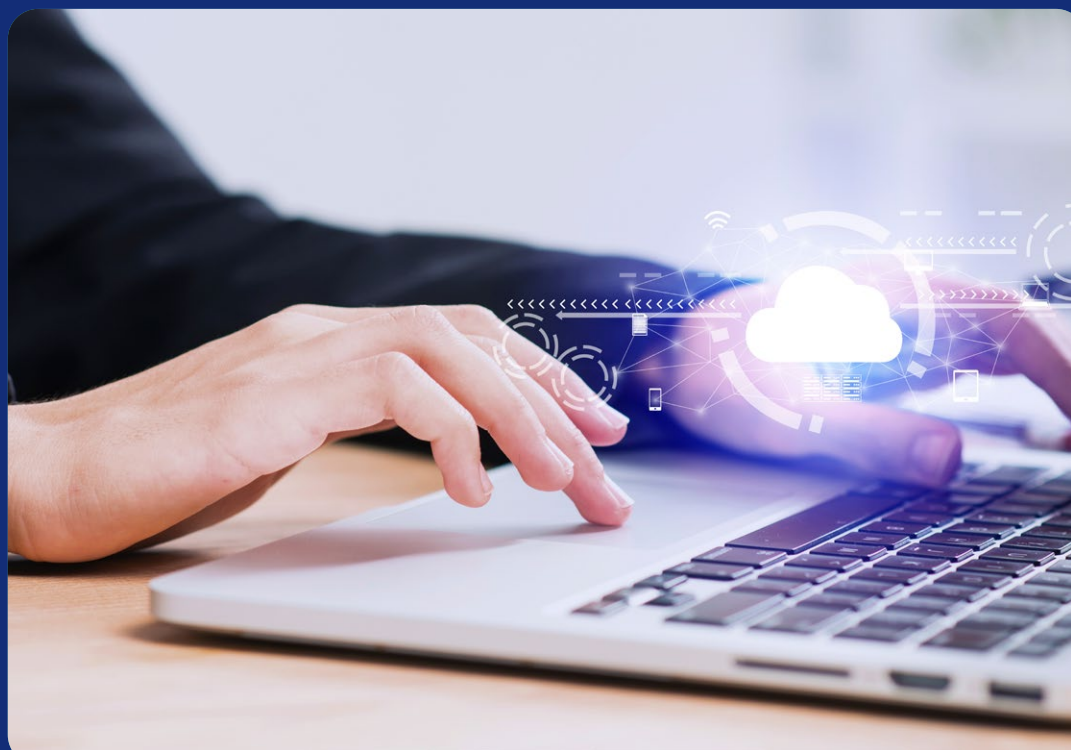
Використання комерційних хмарних технологій для обробки даних державних реєстрів України

IFES Україна | Квітень 2023



Використання комерційних хмарних технологій для обробки даних державних реєстрів України

Розміщення даних із державних реєстрів України у захищеній хмарній інфраструктурі, фізично розміщеній за кордоном, ефективним способом гарантує безпеку реєстрів з огляду на поточні ризики їх знищення чи втрати в ході триваючого збройного конфлікту. Ефективне застосування хмарних технологій сприятиме досягненню цілей цифрової трансформації та забезпечення кібербезпеки національних інформаційних ресурсів, у тому числі, Державного реєстру виборців.

Дослідження надає українським зацікавленим сторонам важливу інформацію за результатами аналізу переваг і ризиків застосування хмарних технологій, підходів до оцінки таких ризиків, подає огляд правової бази використання комерційних хмарних технологій в окремих країнах, що сприятиме визначенню оптимальної моделі з побудови більш стійкої критичної інформаційної інфраструктури України.

Також сформульовано рекомендації щодо розробки національної хмарної стратегії України, проектних та управлінських вимог для розбудови захищеної урядової хмарної інфраструктури та захисту персональних даних державних реєстрів України.

Використання комерційних хмарних технологій для обробки даних державних реєстрів України

Автори:

Андрій Пазюк, Тетяна Слабко

У частині механізмів взаємодії із провайдерами хмарних послуг, з метою висвітлення кращих практик (без рекомендацій конкретних комерційних рішень) дослідження надавалось для рецензування Amazon Web Services, Google, Microsoft. Люб'язно надана експертна думка Amazon Web Services була взята до відома при уточненні технічних формулювань в резюме публікації

Подяка за організаційний внесок та рецензування Ігорю Ткаченку, Михайлу Горкуші та Катерині Зименко

Ця публікація була розроблена Міжнародною фундацією виборчих систем (IFES) за підтримки Агентства США з міжнародного розвитку (USAID), Міністерства міжнародних справ Канади та британської допомоги від уряду Великої Британії. Будь-які думки, викладені в цьому документі, належать авторам і не обов'язково відображають погляди USAID чи Уряду Сполучених Штатів, Міністерства міжнародних справ Канади чи Уряду Канади, та Уряду Великої Британії.

USAID ВІД АМЕРИКАНСЬКОГО НАРОДУ

In partnership with Canada

UKaid from the British people

Міжнародна фундація виборчих систем IFES

Про IFES Україна

В Україні зусилля IFES спрямовані на зміцнення демократичного прогресу за підтримки Агентства США з міжнародного розвитку, Міністерства міжнародних справ Канади та британської допомоги від уряду Великої Британії. Станом на сьогодні, результатами наших зусиль є:

- забезпечення вільних, чесних та інклюзивних виборів;
- просування політичної доброчесності;
- посилення цифрової трансформації та кібербезпеки;
- забезпечення політичних і виборчих прав усіх українців;
- розвиток поінформованості й залученості громадян.

Зміст

Резюме

Використання комерційних хмарних технологій для обробки даних державних реєстрів України потребує **розроблення і схвалення національної хмарної стратегії, удосконалення законодавства, а також розвитку спроможностей державного сектору управляти процесами хмарної трансформації.**

Питання, що вбачається доцільним врегулювати при формуванні політики у сфері хмарних послуг:

- Закріпити принцип «насамперед хмарні технології» (Cloud First) для проектів з розвитку цифрової інфраструктури, але з урахуванням потреби узгодження верхньорівневих цілей і практичності застосування.
- Запропонувати методику оцінки ризиків при впровадженні хмарних технологій, трирівневу систему оцінки впливу (низький, помірний, високий) на безпеку, переглянути відповідно систему класифікації інформації («службова», «таємна», «цілком таємна») у відповідності з міжнародними стандартами та найкращими практиками.
- Визначити особливості закупівлі хмарних послуг державними установами, можливо через централізовану закупівельну організацію, уповноважену Кабінетом Міністрів України.
- Встановити стандартизовані чіткі вимоги до угоди про рівень послуг (SLA) щодо розмежування відповідальності за безпеку між користувачами і надавачами, підзвітності і контролю за операціями з даними, включаючи дотримання вимог Загального регламенту із захисту данних (GDPR), усунення невідповідностей надавачами хмарних послуг.
- Забезпечити державні установи необхідним навчанням та ресурсами для ефективного та безпечного використання хмарних послуг. Використати наявні тренінгові курси, що пропонуються постачальниками хмарних послуг.
- Створити стимули для надавачів хмарних послуг щодо розташування центрів обробки даних в Україні для підтримки розвитку національної хмарної екосистеми. Застосування хмарних послуг має бути включено в національні і регіональні плани та програми з протидії загрозам критичній інфраструктурі, включаючи аварійні плани, плани реагування на кризові ситуації, плани відновлення об'єктів критичної інфраструктури.
- Розробити чіткий план впровадження проекту та план «міграції у хмари», включаючи терміни, бюджет та показники продуктивності (KPI). Залучати досвідчених постачальників хмарних послуг для розробки відповідних планів впровадження.
- Залучити представників уряду, цифрової індустрії, включаючи постачальників хмарних послуг, стратегічної промисловості, банківсько-фінансового сектору та громадянського експертного середовища, щоб зрозуміти їхні погляди на проблему та досягти консенсусу щодо того, як рухатися вперед.

Консультації та публічні слухання можуть допомогти забезпечити, що будь-які зміни у законодавстві є обґрунтованими та враховують потреби всіх зацікавлених сторін.

Термінологія

безпека як послуга	послуга з кіберзахисту (кібербезпекова послуга), що надається користувачу хмарних послуг з використанням хмарних ресурсів
гібридна хмара	хмарна інфраструктура, що є композицією з двох або більше різних хмарних інфраструктур (приватні, колективні або публічні), що є самостійними об'єктами, пов'язаними між собою технологіями, що дозволяють переносити дані або комп'ютерні програми між цими об'єктами
інфраструктура як послуга (IaaS)	хмарна послуга, що полягає у наданні користувачу хмарних послуг обчислювальних ресурсів, ресурсів зберігання або систем електронних комунікацій за допомогою технології хмарних обчислень
користувач хмарних послуг	фізична або юридична особа, яка використовує хмарні послуги для забезпечення власних потреб
надавач хмарних послуг	юридична особа або фізична особа - підприємець, яка надає одну або більше хмарні послуги самостійно або спільно з іншими надавачами хмарних послуг
платформа як послуга (PaaS)	хмарна послуга, що полягає у наданні користувачу хмарних послуг доступу до інфраструктури та наборів комп'ютерних програм (операційних систем, системних комп'ютерних програм, програмних засобів для комп'ютерного програмування, програмних засобів управління базами даних) за допомогою технології хмарних обчислень
приватна (індивідуальна) хмара	хмарна інфраструктура, що підготовлена для використання єдиним користувачем хмарних послуг та контролюється ним
програмне забезпечення як послуга (SaaS)	хмарна послуга, що полягає у наданні користувачу хмарних послуг доступу до прикладних комп'ютерних програм за допомогою технології хмарних обчислень через онлайн-сервіс або комп'ютерні програми-агенти
технологія хмарних обчислень	технологія забезпечення дистанційного доступу на вимогу користувача до хмарної інфраструктури через електронні комунікаційні мережі
хмара (хмарна інфраструктура)	сукупність динамічно розподілюваних та налаштовуваних хмарних ресурсів, що можуть бути оперативно надані користувачу хмарних послуг і вивільнені через глобальну та локальні мережі передачі даних
хмарна послуга	послуга з надання хмарних ресурсів за допомогою технології хмарних обчислень

хмарні ресурси	будь-які технічні та програмні засоби або інші компоненти інформаційної (автоматизованої) системи, доступ до яких забезпечують технології хмарних обчислень, зокрема процесорний час (обчислювальна потужність), місце у сховищах даних, обчислювальні мережі, бази даних і комп'ютерні програми
центр обробки даних	спеціалізований технічний комплекс, що складається з інженерної (системи безперебійного електроживлення, вентиляції, охолодження та регулювання вологості, пожежної безпеки, фізичної охорони), інформаційної, електронної комунікаційної та програмно-апаратної інфраструктури, засоби якого забезпечують або реалізують надання послуг із зберігання та обробки даних, у тому числі, але не обмежуючи: надання хмарних послуг, резервного копіювання даних, передачі даних, оренди комунікаційних стійок, послуг хостингу
колективна хмара	хмарна інфраструктура, що поділена між визначеною групою взаємопов'язаних користувачів хмарних послуг, які мають спільні потреби, та контролюється користувачами хмарних послуг самостійно або їх представниками
публічна хмара	хмарна інфраструктура, що потенційно доступна для невизначеного кола користувачів хмарних послуг та контролюється надавачем хмарних послуг
обробка персональних даних	будь-яка дія або сукупність дій з персональними даними з використанням або без використання автоматизованих засобів, зокрема збирання, фіксація, упорядкування, структурування, зберігання, адаптація, зміна, відновлення, ознайомлення, псевдонімізація, профілювання, знеособлення, використання, розкриття шляхом передачі або поширення, або надання доступу у інший спосіб, групування або комбінування, обмеження, видалення або знищення
контролер	будь-яка фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних, а також інші фізичні або юридичні особи, для яких цілі та засоби обробки визначені законом
оператор (процесор)	будь-яка фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який здійснює обробку персональних даних від імені контролера та уповноважена на це ним або законодавством
персональні дані	будь-яка інформація, що стосується фізичної особи, яку ідентифіковано або може бути ідентифіковано

Вступ і методологія

Вступ

У зв'язку із широкомасштабним вторгненням збройних сил російської федерації на територію України 24 лютого 2022 року виникли високі ризики фізичного знищення і втручання у роботу державних реєстрів, порушення цілісності, конфіденційності і доступності інформації в них.

Напередодні та під час цих трагічних подій, на офіційні веб-сайти, національні електронні комунікаційні системи й інформаційні ресурси відбувались потужні кібератаки, що серед іншого мали за мету порушити функціонування цифрової інфраструктури, підірвати організаційну стійкість державного управління та обмежити здатність надавати відсіч агресору. Завдяки застосуванню комплексу організаційно-технічних заходів, вдалося не допустити реалізацію зухвалих планів держави-агресора та убезпечити інформаційні системи та інформацію в них від фізичного знищення. Одним з успішних заходів безпеки стало перенесення («міграція») державних інформаційних ресурсів у хмарне середовище комерційних компаній (Amazon AWS, Microsoft Azure, Oracle, Google Cloud).

На той час, законодавче регулювання застосування хмарних технологій в Україні ще не було чинним, але збереження державних реєстрів у такий спосіб було виправданим кроком в умовах крайньої необхідності спричиненої високим рівнем загроз. Подальше застосування хмарних технологій під час триваючого збройного конфлікту є цілком закономірним способом забезпечення захисту власником своїх інформаційних систем і ресурсів, що відповідає обов'язкам, покладеним на нього законодавством. У зв'язку з цим, виникають питання урегулювання існуючого стану та подальшого розвитку використання комерційних хмарних технологій для зберігання і обробки даних державних реєстрів України, у тому числі Державного реєстру виборців України.

Міністерство цифрової трансформації України виявило зацікавленість у проведенні оцінки поточного стану та майбутніх перспектив використання комерційних хмарних технологій для обробки даних державних реєстрів України. Це зацікавлення базується на широкому досвіді Міжнародної фундації виборчих систем в Україні (IFES), яка проводить дослідження, аналізи та оцінки у сферах кібербезпеки та цифрової трансформації. Ці дослідження сприяють визначенню актуальних викликів та передових практик правозастосування окремих механізмів в Україні. Проведення такої оцінки сприятиме виявленню ефективних стратегій використання хмарних технологій для досягнення цілей цифрової трансформації та забезпечення кібербезпеки національних інформаційних ресурсів України.

Методологія

Мета цього дослідження – проаналізувати сучасний стан правового регулювання використання комерційних хмарних технологій для обробки даних державних реєстрів України, у тому числі Державного реєстру виборців, і запропонувати рекомендації щодо подальшого розвитку на основі міжнародних стандартів та кращої світової практики.

Дослідження надає українським зацікавленим сторонам важливу загальну інформацію та результати аналізу переваг і ризиків застосування хмарних технологій, підходи до оцінки таких ризиків (на прикладі Норвегії), подає огляд правової бази використання комерційних хмарних технологій для обробки, у тому числі зберігання даних із державних реєстрів України, зокрема Державного реєстру виборців України в хмарній інфраструктурі, фізично розміщеній за кордоном. Наголошується на тому, що розміщення резервних копій баз даних цього реєстру, у тому числі персональних даних за межами

адміністративної території України в захищеній інфраструктурі є одним із способів фізичної сегрегації для гарантування безпеки виборчої архітектури, яким варто скористатися не лише з огляду на поточні ризики їх знищення чи втрати в ході триваючого збройного конфлікту, а як системне рішення з побудови більш стійкої інформаційної інфраструктури.

У дослідженні подається короткий огляд інституційного і регуляторного розвитку застосування хмарних технологій в Європейському Союзі, розглядається хмарна стратегія Європейської Комісії, окреслюються законодавчі напрямки в яких Україні доцільно приділити додаткову увагу для недопущення відставання у темпах інтеграції в загальноєвропейську хмарну екосистему. Подається рекомендація щодо найскорішої Імплементації актів права ЄС (acquis ЄС) у сфері надання хмарних послуг та усунення невідповідностей до початку та в рамках переговорного процесу щодо вступу України до Європейського Союзу.

В огляді міжнародного досвіду впровадження хмарних проектів національного рівня розкриваються особливості обраних підходів різними державами, такими як Естонія, Румунія, Велика Британія, Сінгапур, Ізраїль і Сполучені Штати Америки. Обрання для дослідження саме цих держав обґрунтовується потребою аналізу різних регуляторних моделей, а також вивчення досвіду держав, що мають різні стартові умови. Наприклад, Естонія обрала модель державно-приватного партнерства, створивши консорціум для розгортання урядової хмари. Румунія лише у минулому році розпочала впроваджувати урядову хмарну інфраструктуру, що охоплює увесь державний сектор і передбачає також централізацію державних кібербезпекових функцій, що потенційно обмежує можливості для приватних надавачів хмарних послуг у доступі на ринок. Велика Британія упродовж останніх 13 років демонструє найбільш ліберально-ринковий підхід через щорічні публічні тендери на закупівлю хмарних послуг для державного сектору, не встановлюючи жодних бар'єрів для доступу на ринок хмарних послуг. Унікальність моделі Сінгапуру полягає у використанні хмарних технологій як базової інфраструктури цифрового управління державою, що може за певних застережень розглядатися як зразок для реалізації національних проектів цифрової трансформації України. У свою чергу, Уряд Ізраїлю на виконання нещодавно схваленої хмарної стратегії, за результатами тендерів обрав Google та Amazon Web Services виконавцями проекту з будівництва нових дата-центрів для надання хмарних послуг уряду на публічній, тобто загальнодоступній платформі, що сприятиме розвитку інновацій у хмарних технологіях і сервісах. Такий підхід також може розглядатися для запозичення Україною. Огляд практики регулювання надання хмарних послуг федеральним агенціям в США демонструє модель дозвільного (за умови постійного підтвердження відповідності) допуску провайдерів на ринок, що має як свої переваги, так і недоліки. Отже, порівнюючи різні національні підходи, можна визначити найбільш оптимальну модель для України з огляду на поточні потреби і перспективи розвитку національної хмарної екосистеми.

За результатами аналізу сформульовано рекомендації щодо розробки національної хмарної стратегії України, проектних умов для урядової хмарної інфраструктури, структури проектного менеджменту з розбудови урядової хмарної інфраструктури, вибору моделі «приземлення» хмарних послуг.

Дослідження було виконане у березні 2023 року на основі інформації з відкритих джерел.

1. Вступ до хмарних технологій

Поняття та особливості хмарних обчислень

Хмарні обчислення — це модель для забезпечення повсюдного, зручного мережевого доступу на вимогу користувачів до спільного пулу конфігурованих обчислювальних ресурсів (наприклад, мереж, серверів, сховищ, програм і служб), які можна швидко надати та використати з мінімальними зусиллями керування або взаємодії постачальників послуг.

Документ «Визначення хмарних обчислень NIST» (2011)[1] містить рекомендації Національного інституту стандартів та технологій (NIST) США щодо визначення хмарних обчислень та їхніх характеристик. Цей документ є важливим для розуміння концепції хмарних обчислень та стандартів, які повинні використовуватися в цій сфері.

- 5 характеристик

NIST визначає такі п’ять характеристик хмарних обчислень:

Самообслуговування на вимогу: Споживач може отримати доступ до ресурсів хмарних обчислень за потреби без потреби взаємодії з постачальником послуг. Це означає, що клієнт може замовити і використовувати ресурси, такі як серверний час і мережеве сховище, віддалено через мережу, в той час як постачальник послуг забезпечує автоматичне надання цих можливостей.

Широкий доступ до мережі: Користувачі можуть отримувати доступ до ресурсів хмарних обчислень через мережу та за допомогою стандартних механізмів, що дозволяє використовувати різні клієнтські платформи, такі як мобільні телефони, планшети, ноутбуки та робочі станції.

Об'єднання ресурсів: Ресурси постачальників об’єднуються для обслуговування кількох споживачів, динамічно розподіляючи фізичні та віртуальні ресурси відповідно до потреб користувачів.

Швидка гнучкість: Ресурси можна надавати та вивільняти відповідно до попиту споживачів, що забезпечує швидку та ефективну відповідь на змінювані потреби клієнтів. Крім того, користувачі можуть привласнювати ресурси в будь-якій кількості в будь-який час.

Вимірюване обслуговування: Використання ресурсів відстежується, контролюється та звітується, що забезпечує прозорість як для клієнта, так і для постачальника послуг.

- 3 моделі послуг

У хмарному обчисленні доступні різні сервісні моделі в залежності від потреб користувачів. Три основні моделі - це «програмне забезпечення як послуга» (SaaS), «платформа як послуга» (PaaS) та «інфраструктура як послуга» (IaaS).

SaaS забезпечує клієнтам доступ до програмного забезпечення через мережу Інтернет. Вони не повинні купувати, встановлювати та підтримувати програмне забезпечення на своїх комп'ютерах, оскільки воно вже розміщене на серверах хмарного постачальника.

1 The NIST Definition of Cloud Computing. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

PaaS забезпечує клієнтам необхідне середовище для створення, розгортання та керування своїми власними додатками. Це включає мови програмування, бібліотеки та інструменти для розробки, тестування та підтримки додатків.

IaaS надає клієнтам доступ до обчислювальних ресурсів, таких як сервери, мережі та сховища даних, які можна орендувати замість покупки та підтримки власних серверів у власному центрі обробки даних або серверній кімнаті.

Ці сервісні моделі надають користувачам більшу гнучкість та ефективність при використанні ресурсів, тому що вони можуть вибирати необхідні функції та послуги та оплачувати тільки те, що вони використовують.

Термін «як послуга» також використовується для низки додаткових пропозицій, таких як «безпека як послуга» (SECaaS), «бізнес-процес як послуга (BPaaS), зберігання як послуга» (STaaS), тому часто говорять про «XaaS», «щось як послуга». Більшість із цих пропозицій можна принаймні приблизно віднести до однієї з категорій вище.

- 4 моделі реалізації

Хмарні послуги можна надавати за допомогою чотирьох моделей реалізації: публічна хмара, приватна хмара, колективна хмара і гібридна хмара.

Публічна хмарна інфраструктура забезпечує послуги для відкритого використання широким загалом. При цьому хмара надає стандартні рішення, які доступні для всіх клієнтів, і найбільшими та найвідомішими постачальниками є Google, Amazon і Microsoft. Публічна хмарна інфраструктура може бути використана клієнтами для вирішення різних завдань, від простих до складних. Крім того, публічна хмарна інфраструктура може бути інтегрована з архітектурою постачальників програмного забезпечення, включаючи українських розробників, які надають програмне забезпечення як послугу. Таким чином, підприємства можуть використовувати послуги з публічної хмари навіть якщо це явно не було частиною придбаної послуги.

Приватна хмара – це середовище, яке призначене для виключного використання окремою організацією або групою підприємств. Приватна хмара може бути керована самою організацією, але зазвичай це потребує значних витрат на побудову та підтримку інфраструктури. Тому, якщо організація не є достатньо великою, то вона не зможе досягти такої ж економії масштабу, як у публічній хмарі. Проте приватна хмара може мати певні переваги в порівнянні з публічною хмарою, такі як більша контрольованість та безпека даних, що зберігаються в ній. Також, якщо організація має значні витрати на побудову та підтримку власної інфраструктури, то вона може вирішити зберегти значні кошти на підтримці приватної хмари.

Колективна хмара. Є різновидом приватної хмари, яка надається виключно для використання певною спільнотою споживачів, що мають спільні інтереси, такі як завдання, дотримання єдиних вимог безпеки, галузевого регулювання тощо. Ця інфраструктура може належати, управлятися та керуватися однією або кількома організаціями в спільноті, третьою стороною або їх комбінацією.

Гібридна хмара – це комбінація публічної та приватної хмар, що дозволяє організаціям використовувати кращі рішення з обох світів, залежно від потреб та вимог бізнесу. Гібридна хмара є однією з найбільш перспективних моделей розгортання хмарних послуг. Вона дозволяє підприємствам максимально оптимізувати використання хмарної інфраструктури, комбінуючи переваги публічної та приватної хмари. За допомогою гібридної хмари підприємства можуть зберігати важливі для бізнесу дані та застосунки в локальних мережах, але використовувати загальнодоступні хмарні рішення для забезпечення додаткових ресурсів, забезпечення більшої мобільності та еластичності обчислювальних можливостей. Гібридна хмара також дозволяє підприємствам більш гнучко розгортати та управляти інфраструктурою відповідно до потреб бізнесу.

Переваги і ризики хмарних технологій

Переваги

Переваги використання хмарних технологій, зокрема зменшення витрат на IT та підвищення гнучкості й операційної ефективності, є ключовими причинами, чому все більше урядів і компаній обирають цей тип технологій.

1. **Зменшення витрат на IT.** Використання хмарних технологій дозволяє компаніям уникнути витрат на фізичне обладнання та забезпечення його ефективної роботи. Встановлення, налаштування та обслуговування фізичного обладнання може бути дуже витратним процесом, особливо для невеликих компаній, які можуть не мати достатньої кількості спеціалістів для проведення цих робіт. Використання хмарних технологій дозволяє компаніям уникнути цих витрат та вмінням управляти своїми витратами на IT більш ефективно.

2. **Підвищення гнучкості та операційної ефективності.** Хмарні технології надають компаніям більшу гнучкість та можливість ефективніше виконувати їхні бізнес-операції. Використання хмарних технологій дозволяє компаніям простіше впроваджувати нові функції та додатки, відкладати та збільшувати масштаб ресурсів, що використовуються в їхніх проектах. Крім того, хмарні технології дозволяють компаніям збільшити швидкість виконання операцій та знизити витрати на їх обслуговування, завдяки введенню інструментів самообслуговування та більшій автоматизації процесів.

3. **Інноваційність.** Хмарні технології дозволяють створювати нові продукти та послуги шляхом забезпечення обчислювальної потужності для розробки, скорочення часу їх виконання, надання доступу до найсучасніших технологій, таких як штучний інтелект, машинне навчання та аналітика великих даних, а також швидкого виправлення помилок безпеки та функцій.

4. **Управління ризиками.** Використання хмарних технологій забезпечує ефективний ризик-менеджмент та підвищує стійкість до забезпечення безперервності обслуговування, завдяки удосконаленню управління даними та ризиками кібербезпеки, що знижує ризики для окремих компаній та організацій.

5. **Доступність.** Хмарні технології забезпечують інклюзивність та гендерну рівність, забезпечуючи більший доступ до фінансових продуктів для людей, які раніше не мали такого доступу, а також сприяють різноманітності та конкуренції в галузі.

6. **Екологічність.** Використання хмарних технологій позитивно впливає на клімат, оскільки вони зменшують споживання енергії та викиди вуглецю порівняно з фізичним створенням IT-інфраструктури.

Ризики

Передача даних на аутсорсинг завжди пов'язана з ризиком. Особливі ризики, пов'язані з хмарними обчисленнями:

Втрата контролю над даними. За загальною практикою постачальники хмарних послуг є процесорами (операторами хмарних послуг), а отже, вони повинні діяти повністю відповідно до інструкцій контролера даних, який замовляє розміщення даних у хмарі. Саме контролери даних визначають мету та методи обробки даних процесорами (операторами) даних. Незважаючи на це, іноді процесори (оператори) даних відступають від цього правила і починають здійснювати обробку даних у своїх цілях (як з комерційною, так і некомерційною метою), частіше за все, з метою розвитку своїх сервісів. Це пояснюється високою цінністю даних в сучасному світі. У таких ситуаціях контолер даних, фактично, втрачає важелі впливу на процесора (оператора), не може гарантувати належну реалізацію прав суб'єктам даних, добитися видалення таких даних тощо.

Відсутнє або недостатнє розділення/ізоляція процесів обробки даних різних користувачів. Ключовою особливістю концепції хмарних обчислень є те, що різні абсолютно не зв'язані користувачі можуть розміщувати свої дані в одній хмарі та обробляти їх в одній системі (відома як архітектура з кількома клієнтами). Це збільшує ризик того, що інциденти із даними одного із користувачів хмарних послуг, фактично, матимуть вплив і на інших користувачів. Можливі варіанти інцидентів: втрата доступу до даних, порушення цілісності даних, неавторизована передача даних третім особам. Це може статися внаслідок хакерських атак або атак розподіленої відмови в облуговуванні (DDoS).

Ризики відповідності. У хмарі існує небезпека того, що різні частини набору даних потраплять у різні центри обробки даних по всьому світу. Це може призвести до проблем не лише з точки зору захисту та безпеки даних, але й у зв'язку з іншими правовими вимогами (зобов'язання безпечного зберігання, тягар доведення, конфіденційність тощо). Компанії та державні органи, які використовують послуги хмарних обчислень, часто недостатньо усвідомлюють той факт, що відповідальність за виконання вимог захисту даних лежить на них, а не на провайдері, який зберігає дані на хмарному сервері або обробляє дані в хмарі.

Доступ іноземних органів до даних. Через глобальну мережу та її віртуальний характер місцезнаходження даних часто невідоме користувачу. Це особливо вірно у випадку публічних хмар. Користувач хмари, як відповідальний контролер файлу даних, не знає, де саме в хмарі зберігаються та обробляються її дані. Тож може виникнути ситуація, за якої дані будуть фізично знаходитися на території держав, рівень захисту даних в яких не відповідає належному, є ризики безперешкодного доступу до даних місцевими органами державної влади, зокрема, правоохоронними органами.

Ефект блокування. Ще одним ризиком є ступінь залежності від постачальника хмарних послуг і відсутність портативності та сумісності. Іншими словами, оскільки стандартизовані технології та інтерфейси не використовуються, дані не можуть бути передані назад у власну IT-систему компанії або перенесені до іншого хмарного постачальника - або, принаймні, це можна зробити лише за великі кошти.

ОЦІНКА РИЗИКІВ. ПРИКЛАД НОРВЕГІЇ

У червні 2014 року Уряд призначив комісію з вивчення цифрової вразливості суспільства (Комісія Лісне). Комісія представила свій Звіт[2] Міністру юстиції та громадської безпеки Норвегії 30 листопада 2015 року. Деякі з питань, пов'язаних із хмарними обчисленнями, обговорюваними у звіті:

- Великі відомі постачальники хмарних обчислень часто можуть запропонувати кращу безпеку, ніж багато малих організацій. Звичайно, це буде залежати від постачальника. Користувач несе відповідальність за оцінку того, чи є інформація, яку він має намір зберігати в хмарі, вразливою у разі передачі за межі юрисдикції Норвегії, і повинен зважити наслідки та ризик проти переваг.
- Урядові органи влади не повинні ускладнювати впровадження практичних і економічно ефективних технологій, доки існують достатньо безпечні рішення. Важливо, щоб норвезьке законодавство не перешкоджало підвищенню конкурентоспроможності.
- Розділ 9 Закону про державні архіви, який визначає, що архіви не можуть бути переміщені за межі країни, був введений понад 20 років тому, і тому не враховує сучасні технологічні розробки та потреби.

Рекомендації Комісії:

Інформацію можна розділити на три категорії:

1. Інформація, яку слід зберігати лише в Норвегії.
2. Інформація, яку можна зберігати за кордоном, але яку можна повернути до Норвегії, якщо необхідно, відповідно до певних умов.
3. Інформація, яка може зберігатися за кордоном без певних умов.

Категорія 1: інформація, яка повинна зберігатися лише на території та під юрисдикцією Норвегії, стосується особливо секретної інформації. Комісія робить висновок, що кожен сектор повинен оцінити, яка інформація підпадає під відповідні категорії. Комісія також наголошує, що секторам у багатьох випадках буде важко координувати роботу один з одним, тому існує потреба в стандартах і вказівках для всіх секторів.

Комісія наголосила на необхідності гармонізації практики нагляду в усіх секторах. Ця робота повинна включати більше уваги використанню незалежних аудитів.

2 Cloud Computing Strategy for Norway. https://www.regjeringen.no/contentassets/4e30afec51734d458596e723c0bdea0e/cloud_computing_strategy.pdf

2. Правове регулювання використання хмарних технологій для обробки державних інформаційних ресурсів в Україні

Організаційно-правові основи застосування хмарних технологій

Національна економічна стратегія на період до 2030 року[3] визнає важливість розвитку хмарних послуг для економіки України і встановлює кілька конкретних кроків, які мають бути зроблені для сприяння цьому розвитку. Зокрема, важливим є закріплення принципу «насамперед хмарні технології» (Cloud First), що означає, що при розробці будь-якої нової інформаційної системи або розширенні наявної системи, перевага має надаватися хмарним технологіям. Ставиться за мету підвищення рівня використання хмарних технологій і віртуалізації для 90 відсотків бізнесу. Це допоможе підвищити ефективність та знизити витрати на обслуговування інформаційних систем.

Забезпечення сприятливих умов для побудови великих центрів обробки даних для хмарних сервісів є також важливим кроком. Це може забезпечити необхідну інфраструктуру для розширення хмарних послуг в Україні. Надання підтримки експорту послуг хмарних обчислень і хмарних сховищ також є важливим кроком для забезпечення зростання української економіки та її конкурентоспроможності на міжнародному ринку. Важливим елементом стратегії є залучення міжнародних інвесторів і високотехнологічних компаній, таких як Microsoft, Amazon, Alphabet, Alibaba, Facebook, Apple, для побудови інфраструктури хмарних сервісів в Україні.

У Стратегії зазначається необхідність нормативного забезпечення можливості використання хмарних послуг і зазначається, що «відсутність ефективної системи регулювання хмарних сервісів зменшує потенціал України на одному з найдинамічніших цифрових ринків». Також у Стратегії розвитку фінтеху в Україні до 2025 р.[4] і Стратегії розвитку фінансового сектору України до 2025 р.[5] заплановано прийняття спеціального законодавства щодо хмарних послуг у фінансовому секторі.

Закон України «Про хмарні послуги» від 17 лютого 2022 року № 2075-IX[6] набув чинності 16 вересня 2022 року. Його мета – створення умов для обробки та захисту даних при використанні технології хмарних обчислень, визначення особливостей використання хмарних послуг органами державної

3 Постанова Кабінету Міністрів України «Про затвердження Національної економічної стратегії на період до 2030 року». https://zakon.rada.gov.ua/go/179-2021-%D0%BF

4 Стратегія розвитку фінтеху в Україні до 2025 року. https://bank.gov.ua/ua/files/DDWIAwXTdqjdClp

5 Стратегія розвитку фінансового сектору України до 2025 року. https://bank.gov.ua/admin_uploads/article/Strategy_FS_2025.pdf?v=4

6 Закон України «Про хмарні послуги». https://zakon.rada.gov.ua/laws/show/2075-20#Text

влади, а також більш ефективне використання державних ресурсів шляхом впровадження новітніх технологій.

Закон визначає правові відносини, що виникають при наданні хмарних послуг, та встановлює особливості використання хмарних послуг органами державної влади, органами влади Автономної Республіки Крим, органами місцевого самоврядування, військовими формуваннями, утвореними відповідно до законів України, державними підприємствами, установами та організаціями, суб'єктами владних повноважень та іншими суб'єктами, яким делеговані такі повноваження.

Закон визначає:

- поняття «хмарних обчислень», «хмарних послуг», «надавача хмарних послуг», «користувача хмарних послуг», «хмарних ресурсів», «центр обробки даних (ЦОД)»;
- види хмарних послуг;
- використання хмарних послуг;
- учасників відносин у сфері хмарних послуг;
- державне управління і регулювання при наданні хмарних послуг;
- повноваження регулятора комунікаційних послуг;
- вимоги до надавача хмарних послуг та/або послуг центру обробки даних;
- ведення переліку надавачів хмарних послуг та/або послуг центру обробки даних;
- надання хмарних послуг та/або послуг центру обробки даних;
- порядок надання хмарних послуг, пов'язаних з обробкою державних інформаційних ресурсів або інформації з обмеженим доступом;
- обробку персональних даних при наданні хмарних послуг та/або послуг центру обробки даних;
- захист інформації при наданні хмарних послуг та/або послуг центру обробки даних;
- міжнародне співробітництво.

Частиною першою статті 6 Закону визначено, що організаційну систему державного управління і регулювання при наданні хмарних послуг становлять: 1) Кабінет Міністрів України; 2) регулятор комунікаційних послуг; 3) центральний орган виконавчої влади, що формує та реалізує державну політику при наданні хмарних послуг; 4) орган, уповноважений здійснювати контроль за додержанням законодавства про захист персональних даних; 5) Міністерство оборони України; 6) Національний банк України; 7) Центральна виборча комісія.

Положеннями статті 7 Закону встановлено, що регулятор комунікаційних послуг і є центральним органом виконавчої влади, що формує та реалізує державну політику при наданні хмарних послуг. **Водночас, закон не визначив повноваження Центральної виборчої комісії як учасника відносин у сфері хмарних послуг**.

Згідно з частиною другою статті 8 закону для надання хмарних послуг та/або послуг центру обробки даних публічним користувачам та/або критично важливим об'єктам інфраструктури відомості про надавачів хмарних послуг та/або послуг центру обробки даних мають бути внесені до переліку.

Відповідно до частини першої статті 12 Закону Кабінет Міністрів України встановлює порядок надання хмарних послуг та/або послуг центру обробки даних, пов'язаних з обробкою державних інформаційних

ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що базується на принципах інтероперабельності та збереження конкуренції, і визначає порядок:

- обов'язкового резервного копіювання та збереження резервних копій у незалежних системах;
- передачі даних від користувача хмарних послуг до надавача хмарних послуг та/або послуг центру обробки даних для забезпечення надання хмарних послуг, а також від надавача хмарних послуг до користувача хмарних послуг;
- передачі даних від одного надавача хмарних послуг та/або послуг центру обробки даних до іншого;
- надання інформації, необхідної для оцінювання безпеки мережевих та інформаційних систем надавачів хмарних послуг та/або послуг центру обробки даних, у тому числі документально встановленої політики безпеки.

Частина друга статті 12 Закону встановлює вимоги щодо положень, які має містити порядок надання хмарних послуг та/або послуг центру обробки даних. Такий порядок має включати:

- вимоги щодо передачі даних у структурованому вигляді, загальновживаних та машинозчитувальних форматах;
- вимогу до обсягу інформації щодо процесів, технічних вимог, строків та платежів, що застосовуються у разі переходу до іншого надавача хмарних послуг та/або послуг центру обробки даних або відмови від хмарних послуг, яка має бути надана користувачу хмарних послуг у чіткій та доступній формі до визначення переможця процедури закупівлі (спрощеної процедури закупівлі);
- підходи, що полегшують порівняння хмарних послуг та/або послуг центру обробки даних та хмарної інфраструктури, що включають, зокрема інформацію про управління якістю, управління інформаційною безпекою, управління безперервністю надання послуг, про оцінку впливу на довкілля.

З метою реалізації положень Закону, **потребує визначення центральний орган виконавчої влади, що формує та реалізує державну політику при наданні хмарних послуг.** Саме на цей орган покладатиметься розроблення та внесення на розгляд Уряду відповідних проектів актів, що відповідно до пункту 1 частини третьої статті 16 Закону доручено виконати Кабінету Міністрів України:

- приводить свої нормативно-правові акти у відповідність із Законом;
- визначає структуру, порядок формування та використання електронних каталогів хмарних послуг та/або послуг центру обробки даних;
- визначає вимоги до надавачів хмарних послуг та/або послуг центру обробки даних, яким надавач хмарних послуг має відповідати для внесення до переліку за відповідними видами послуг, та порядок підтвердження відповідності цим вимогам;
- встановлює порядок надання хмарних послуг та/або послуг центру обробки даних, пов'язаних з обробкою державних інформаційних ресурсів;
- визначає порядок підготовки пропозицій щодо використання хмарних послуг та/або послуг центру обробки даних органами державної влади, органами влади Автономної Республіки Крим та їх розгляду;
- забезпечує перегляд та приведення міністерствами та іншими центральними органами виконавчої влади їх нормативно-правових актів у відповідність із Законом.

Крім того, на Кабінет Міністрів України покладено також інші завдання щодо затвердження підзаконних нормативно-правових актів щодо:

- вимог у сфері електронних довірчих послуг за допомогою технології хмарних обчислень (ч. 1 статті 4 Закону);
- типового договору про надання хмарних послуг та/або послуг центру обробки даних публічному користувачу та об'єкту критичної інформаційної інфраструктури (ч. 2 статті 10 Закону);
- визначення особливостей порядку застосування технології хмарних обчислень та надання хмарних послуг та послуг центру обробки даних з питань національної безпеки у воєнній і оборонній сферах, у тому числі питання, пов'язані із зверненням за одержанням хмарних послуг в інтересах оборони та порядок отримання хмарних послуг, покладено на Міністерство оборони України (ч. 4 статті 10 Закону).

Стаття 8 Закону вимагає від надавача хмарних послуг та/або послуг центру обробки даних виконання низки вимог. Надавач повинен:

- надавати державному органу, призначеному для формування та реалізації державної політики у сфері кіберзахисту, інформацію, необхідну для оцінювання безпеки електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, у тому числі документально встановленої політики безпеки;
- усувати будь-яку невідповідність **вимогам, затвердженим регулятором комунікаційних послуг**.

Відповідно до статті 14 цього Закону надавач хмарних послуг та/або послуг центру обробки даних забезпечує та створює належні умови для захисту даних у системі хмарних обчислень у порядку, визначеному законодавством України та договором між сторонами. На вимогу користувача хмарних послуг та/або у порядку, визначеному договором, надавач хмарних послуг та/або послуг центру обробки даних надає інформацію щодо захисту інформації в системі хмарних обчислень від внутрішніх та зовнішніх загроз, кібератак.

Розглянемо далі вимоги законодавства України щодо захисту інформації при використанні хмарних технологій.

Захист інформації в державних реєстрах України при використанні хмарних технологій

Закон України «Про публічні електронні реєстри» (від 18.11.2021 № 1907-IX)[7] є основним документом, що регулює питання створення, збереження та захисту реєстрової інформації в Україні. Цей закон повністю узгоджений з Законом України «Про захист інформації в інформаційно-комунікаційних системах» (№ 1089-IX від 16.12.2020)[8], який встановлює вимоги щодо захисту інформації в інформаційних системах.

Відповідно до статті 9 цього Закону відповідальність за забезпечення захисту інформації в системі покладається на власника системи.

Згідно з цим законодавством, збереження реєстрової інформації здійснюється з обов'язковим застосуванням засобів резервного копіювання та хеш-логування (ч. 3 статті 18), а створення реєстру

7 Закон України «Про публічні електронні реєстри». https://zakon.rada.gov.ua/go/1907-20

8 Закон України «Про електронні комунікації». https://zakon.rada.gov.ua/laws/show/1089-20#n2339

забезпечується застосуванням сертифікованих засобів технічного і криптографічного захисту інформації (ч. 6 статті 26). Закон також передбачає проведення державної експертизи комплексної системи захисту інформації (далі – КСЗІ), що використовується для обробки державних інформаційних ресурсів або інформації з обмеженим доступом (стаття 8).

Відповідно до частини четвертої статті 8 Закону України «Про захист інформації в інформаційно-комунікаційних системах»:

Державні інформаційні ресурси та інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, крім державної таємниці, службової інформації та інформації з державних і єдиних реєстрів, створення та забезпечення функціонування яких визначені законом, можуть оброблятися в системі без застосування комплексної системи захисту інформації у разі виконання всіх таких умов:

- підтвердження відповідності системи управління інформаційною безпекою за результатами процедури з оцінки відповідності національним стандартам України щодо систем управління інформаційною безпекою, яка проведена органом з оцінки відповідності, акредитованим національним органом України з акредитації чи національним органом з акредитації іноземної держави, якщо і національний орган України з акредитації, і національний орган з акредитації іноземної держави є членами міжнародної або регіональної організації з акредитації та/або уклали з такою організацією угоду про взаємне визнання щодо оцінки відповідності;
- використання для захисту інформації в системі засобів криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації або документ про відповідність, виданий за результатами сертифікації таких засобів відповідно до Закону України «Про технічні регламенти та оцінку відповідності»;
- жодний з елементів системи не розташований, а власник такої системи або його офіційний представник не є юридичною особою (її представником), зареєстрованою на територіях України, на яких органи державної влади України тимчасово не здійснюють своїх повноважень, на території держави, визнаної Верховною Радою України державою-агресором, на території держави, щодо якої застосовані санкції відповідно до Закону України «Про санкції», або на території держави, яка входить до митного союзу з такими державами;
- власник системи або його представник, який надає послуги з використанням системи, елементи якої розміщуються поза межами України, є юридичною особою, зареєстрованою в Україні, або має свого офіційного представника в Україні;
- виконання особливих вимог, встановлених Кабінетом Міністрів України до забезпечення захисту інформації в системах залежно від категорії державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, що обробляються.

Стаття 8 Закону України «Про хмарні послуги» (від 17 лютого 2022 року N° 2075-IX)[9] вимагає від надавача хмарних послуг та/або послуг центру обробки даних виконання низки вимог. **Надавач хмарних послуг та/або послуг центру обробки даних повинен вжити відповідних пропорційних технічних та організаційних заходів для управління ризиками, що виникають для безпеки електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг.**

9 Закон України «Про хмарні послуги». https://zakon.rada.gov.ua/laws/show/2075-20

Такі заходи мають забезпечувати рівень безпеки електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, які використовуються для надання хмарних послуг, що відповідає ризику, який виник, та враховувати такі елементи: безпеку систем та устаткування; врегулювання інцидентів; управління безперервністю бізнесу; моніторинг, аудит та випробування; відповідність міжнародним стандартам.

Надавач хмарних послуг та/або послуг центру обробки даних без необґрунтованої затримки повинен повідомляти регулятора комунікаційних послуг та CERT-UA про будь-який інцидент, який має значний негативний вплив на надання хмарної послуги та/або послуг центру обробки даних, у порядку, затвердженому регулятором комунікаційних послуг.

Надавач хмарних послуг та/або послуг центру обробки даних повинен:

- надавати державному органу, призначеному для формування та реалізації державної політики у сфері кіберзахисту, інформацію, необхідну для оцінювання безпеки електронної комунікаційної мережі, електронної комунікаційної послуги та інформаційних систем, у тому числі документально встановленої політики безпеки;
- усувати будь-яку невідповідність вимогам, затвердженим регулятором комунікаційних послуг.

На думку Головного юридичного управління Апарату Верховної Ради України (№ 07/02-2021/381368 від 07.12.2021)[10], в цьому положенні фактично йдеться про ліцензування виду господарської діяльності. Вочевидь, зазначені положення потребують узгодження зі статтею 12 Господарського кодексу України та вимогами, встановленим Законом України «Про ліцензування видів господарської діяльності».

Надавач хмарних послуг та/або послуг центру обробки даних публічним користувачам та критично важливим об'єктам інфраструктури до початку надання цих послуг повинен повідомити публічному користувачу та критично важливим об'єктам інфраструктури інформацію про ризики безпеки інформації у зв'язку з її обробленням у системі хмарних обчислень.

Відповідно до статті 14 цього Закону надавач хмарних послуг та/або послуг центру обробки даних забезпечує та створює належні умови для захисту даних у системі хмарних обчислень у порядку, визначеному законодавством України та договором між сторонами. На вимогу користувача хмарних послуг та/або у порядку, визначеному договором, надавач хмарних послуг та/або послуг центру обробки даних надає інформацію щодо захисту інформації в системі хмарних обчислень від внутрішніх та зовнішніх загроз, кібератак.

Прикінцевими положеннями Закону України «Про хмарні послуги» було виключено друге речення частини п'ятої статті 6 Закону України «Про захист персональних даних»[11], яким заборонялася обробка персональних даних, вимога щодо захисту яких встановлена законом, за допомогою технології хмарних обчислень та ЦОД, що розміщені за межами адміністративно-територіальних кордонів України.

Використання хмарних ресурсів та центрів обробки даних, що розташовані за межами України, було врегульовано Законом України «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів» № 2130-IX від 15.03.2022[12].

10 Зауваження до проекту Закону України про хмарні послуги. https://itd.rada.gov.ua/billinfo/Bills/pubFile/1093575

11 Закон України «Про захист персональних даних». https://zakon.rada.gov.ua/laws/show/2297-17

12 Закон України «Про внесення змін до деяких законів України щодо забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів». https://zakon.rada.gov.ua/go/2130-20

Відповідно до цього Закону, власники систем для забезпечення належного функціонування систем та захисту інформації, що обробляється в них:

- створюють резервні копії державних інформаційних ресурсів та систем із дотриманням встановлених для таких ресурсів та систем вимог щодо їх захисту, цілісності та конфіденційності;
- забезпечують створення резервних копій державних інформаційних ресурсів та систем на окремих фізичних носіях у зашифрованому вигляді та їх подальшу передачу (переміщення) для зберігання в установленому законодавством порядку, у тому числі за межами України (зокрема в закордонних дипломатичних установах України), протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування;
- забезпечують в установленому законодавством порядку передачу (переміщення) державних інформаційних ресурсів та їх резервних копій для розміщення на хмарних ресурсах та/або в центрах обробки даних, розташованих за межами України, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування.

Відповідно до частини другої статті 38 Закону України «Про публічні електронні реєстри» дозволяється ведення публічних електронних реєстрів за допомогою хмарних ресурсів та/або центрів обробки даних, у тому числі розміщених за межами України, протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування. Порядок передачі, зберігання, функціонування та доступу до відповідних публічних електронних реєстрів[13] встановлюється Кабінетом Міністрів України.

Розміщення систем та зберігання резервних копій державних інформаційних ресурсів та систем на територіях України, на яких органи державної влади України тимчасово не здійснюють свої повноваження, територіях держав, визнаних Верховною Радою України державами-агресорами, територіях держав, щодо яких застосовані санкції відповідно до Закону України «Про санкції»[14], та територіях держав, які входять до митних та воєнних союзів з такими державами, забороняється.

Постановою КМУ від 12 березня 2022 р. № 263 «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану»[15] передбачається, що на період дії воєнного стану міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, установи, організації, що належать до сфери їх управління, для забезпечення належного функціонування інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, публічних електронних реєстрів, володільцями (держателями) та/або адміністраторами яких вони є, та захисту інформації, що обробляється в них, можуть вживати таких додаткових заходів:

- розміщувати державні інформаційні ресурси та публічні електронні реєстри на хмарних ресурсах та/або в центрах обробки даних, що розташовані за межами України, та реєструвати доменні імена у домені gov.ua для такого розміщення;
- створювати додаткові резервні копії державних інформаційних ресурсів та публічних електронних реєстрів з дотриманням установлених для таких ресурсів вимог щодо цілісності, конфіденційності та доступності;
- зупиняти, обмежувати роботу інформаційних, інформаційно-комунікаційних та електронних комунікаційних систем, а також публічних електронних реєстрів.

13 Постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування державних інформаційних ресурсів». https://zakon.rada.gov.ua/laws/show/1500-2022-%D0%BF

14 Закон України «Про санкції». https://zakon.rada.gov.ua/laws/show/1644-18

15 Постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування інформаційно-комунікаційних систем, електронних комунікаційних систем, публічних електронних реєстрів в умовах воєнного стану». https://zakon.rada.gov.ua/laws/show/263-2022-%D0%BF#Text

Міністерства, інші центральні та місцеві органи виконавчої влади, державні та комунальні підприємства, установи, організації, що належать до сфери їх управління, можуть використовувати хмарні ресурси та/або центри обробки даних, що розташовані за межами державного кордону України, на безоплатній або платній основі.

Міністерствам, іншим центральним та місцевим органам виконавчої влади доручено **протягом шести місяців після припинення чи скасування воєнного стану припинити здійснення вищезазначених заходів, невідкладно повідомити про припинення вжиття зазначених заходів** Адміністрації Державної служби спеціального зв'язку та захисту інформації та Міністерству цифрової трансформації.

Постановою Кабінету Міністрів України від 30 грудня 2022 р. № 1500[16] затверджено:

1) Порядок передачі, збереження, функціонування та доступу до державних інформаційних ресурсів (публічних електронних реєстрів) та їх резервних копій, розміщених на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України;

2) Порядок укладення договорів володільцями інформації — власниками (держателями) державних інформаційних ресурсів (публічних електронних реєстрів) про технічне адміністрування відповідних реєстрів з іноземними компаніями, організаціями — постачальниками послуг з надання хмарних ресурсів (надавачами хмарних послуг), утвореними відповідно до законодавства інших держав, та/або їх зареєстрованими (акредитованими або легалізованими) відповідно до законодавства України філіями, представництвами та іншими відокремленими підрозділами з місцезнаходженням на території України;

3) Перелік видів державних інформаційних ресурсів та систем, щодо яких може здійснюватися резервне копіювання — бази даних, національні електронні інформаційні ресурси, публічні електронні реєстри, інформаційні (автоматизовані) системи, інформаційно-комунікаційні системи.

Порядок, згаданий першим, визначає механізм передачі (переміщення) державних інформаційних ресурсів (публічних електронних реєстрів), які не містять службової інформації та інформації, що становить державну таємницю, та їх резервних копій для розміщення на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України, забезпечення збереження, функціонування та доступу до таких інформаційних ресурсів.

Цей Порядок протягом періоду дії правового режиму воєнного стану в Україні та шести місяців після його припинення чи скасування регулює відносини володільців інформації - власників (держателів) державних інформаційних ресурсів, які виявили бажання (намір) розмістити державні інформаційні ресурси та їх резервні копії на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України.

Пунктом 7 Порядку визначено вимогу щодо наявності у постачальника послуг (надавача хмарних послуг або ресурсів у центрах обробки даних), до якого передаються (переміщуються) державні інформаційні ресурси або їх резервні копії, документа про відповідність впровадження системи інформаційної безпеки міжнародним стандартам.

Відповідно до п. 8 Порядку замовники обробляють державні інформаційні ресурси, розміщені на хмарному ресурсі та/або центрі обробки даних, що розташований за межами України, із застосуванням системи управління інформаційною безпекою або комплексної системи захисту інформації (КСЗІ).

Пунктом 9 Порядку встановлено вимоги щодо необхідності оцінки замовником зміни умов функціонування ІКС та за потреби модернізації КСЗІ. Під час переміщення до хмарних ресурсів та/

16 Постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування державних інформаційних ресурсів». https://www.kmu.gov.ua/npas/deiaki-pytannia-zabezpechennia-funktsionuvannia-derzhavnykh-informatsiinykh-t301222

або центрів обробки даних, що розташовані за межами України, інформаційно-комунікаційної системи, яка має чинний атестат відповідності КСЗІ з підтвердженою відповідністю, атестат відповідності КСЗІ інформаційно-комунікаційної системи не втрачає чинності за таких умов: технологія обробки інформації не змінилася; програмний склад інформаційно-комунікаційної системи, що виконує функції захисту інформації, відповідає оціненим проектним рішенням КСЗІ; постачальник послуг має документ про відповідність впровадження системи інформаційної безпеки міжнародним стандартам.

В інших випадках здійснюються заходи з модернізації КСЗІ відповідно до законодавства України у сфері захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах.

Протягом шести місяців після припинення чи скасування правового режиму воєнного стану в Україні замовники, з якими укладено договір відповідно до пункту 3 цього Порядку, повинні забезпечити:

- **припинення використання відповідних хмарних ресурсів та центрів обробки даних, що розміщені за межами України, на яких функціонують та зберігаються державні інформаційні ресурси та їхні резервні копії;**
- **функціонування державних інформаційних ресурсів та зберігання їх резервних копій на території України.**

Правилами забезпечення захисту інформації в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах, затверджених постановою КМУ від 23.03.2006 № 373[17], встановлено зокрема таке:

- захисту в системі підлягає відкрита інформація, яка належить до державних інформаційних ресурсів, а також відкрита інформація про діяльність суб'єктів владних повноважень, військових формувань, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається електронними комунікаційними мережами;
- відкрита інформація під час обробки в системі повинна зберігати цілісність, що забезпечується шляхом захисту від несанкціонованих дій, які можуть призвести до її випадкової або умисної модифікації чи знищення;
- усім користувачам повинен бути забезпечений доступ до ознайомлення з відкритою інформацією. Модифікувати або знищувати відкриту інформацію можуть лише ідентифіковані та автентифіковані користувачі, яким надано відповідні повноваження;
- спроби модифікації чи знищення відкритої інформації користувачами, які не мають на це повноважень, неідентифікованими користувачами або користувачами з не підтвердженою під час автентифікації відповідністю пред'явленого ідентифікатора повинні блокуватися;
- у системі здійснюється обов'язкова реєстрація:
  - результатів ідентифікації та автентифікації користувачів;
  - результатів виконання користувачем операцій з обробки інформації;
  - спроб несанкціонованих дій з інформацією;
  - фактів надання та позбавлення користувачів права доступу до інформації та її обробки;
  - результатів перевірки цілісності засобів захисту інформації.

17 Постанова Кабінету Міністрів України «Про внесення змін до постанов Кабінету Міністрів України від 23 червня 2003 р. № 953 і від 20 серпня 2003 р. № 1307». https://zakon.rada.gov.ua/laws/show/996-2006-%D0%BF#Text

- забезпечується можливість проведення аналізу реєстраційних даних виключно користувачем, якого уповноважено здійснювати управління засобами захисту інформації і контроль за захистом інформації в системі (адміністратор безпеки);
- реєстрація здійснюється автоматичним способом, а реєстраційні дані захищаються від модифікації та знищення користувачами, які не мають повноважень адміністратора безпеки;
- реєстрація спроб несанкціонованих дій з інформацією, що становить державну таємницю, і службовою інформацією повинна супроводжуватися повідомленням про них адміністратору безпеки (відповідальній особі);
- ідентифікація та автентифікація користувачів, надання та позбавлення їх права доступу до інформації та її обробки, контроль за цілісністю засобів захисту в системі здійснюється автоматизованим способом;
- автентифікація користувачів у системі здійснюється відповідно до вимог статті 17 Закону України «Про електронні довірчі послуги» та інших нормативно-правових актів;
- у системі здійснюється контроль за цілісністю програмного забезпечення, яке використовується для обробки інформації, запобігання несанкціонованій його модифікації та ліквідація наслідків такої модифікації;
- контролюється також цілісність програмних та технічних засобів захисту інформації. У разі порушення їх цілісності обробка в системі інформації припиняється;
- захист інформації від несанкціонованих дій (НСД), у тому числі від комп'ютерних вірусів, забезпечується в усіх системах.

Таким чином, загальний перелік вимог до захисту інформації публічних реєстрів є достатньо визначеним. Але захист інформації в ІКС має однозначно забезпечуватися або застосуванням в ній КСЗІ, або СУІБ з підтвердженою відповідністю.

У випадку переходу на використання хмарних сервісів виникає потреба модернізації КСЗІ, що можна було б врегулювати шляхом **визначення типових вимог щодо Стандартних функціональних профілів (СФП) захищеності. При цьому частину цих послуг безпеки з СФП забезпечуватиме надавач хмарних послуг, про що має відповідний атестат. Власнику ж реєстру залишилося б в рамках своєї КСЗІ реалізувати лише ті послуги з визначеного СФП, які не реалізовані надавачем хмарних послуг.**

Потребують розроблення рекомендації (настанови) щодо забезпечення кіберзахисту при використанні хмарних обчислень **на основі міжнародних стандартів та кращих світових практик**.

Перелік міжнародних стандартів та світових практик у сфері хмарних обчислень

ISO/IEC 17788:2014. Інформаційні технології. Хмарні обчислення. Огляд та основні терміни[18];

ДСТУ ISO/IEC 27017:2016 Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки хмарних послуг, що ґрунтуються на ISO/IEC 27002 (ISO/IEC 27017:2015, IDT)[19];

18 Наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» «Про прийняття національних нормативних документів, гармонізованих з міжнародними та європейськими нормативними документами, скасування чинності національних нормативних документів та змін до національних нормативних документів». https://zakon.rada.gov.ua/rada/show/v0428774-17#Text

19 Наказ Державного підприємства «Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості» «Про прийняття національних стандартів України, змін та поправок до національних стандартів України, гармонізованих з міжнародними нормативними документами». https://zakon.rada.gov.ua/rada/show/v0307774-16#Text

Інструкції щодо хмарних обчислень. Рада зі стандартів безпеки даних індустрії платіжних карток / PCI DSS Cloud Computing Guidelines[20], PCI Security Standards Council (2018). PCI DSS Cloud Computing Guidelines, Version 3.0.

NIST IR 8320 (2022)[21]. Апаратно-забезпечена безпека: забезпечення шарованого підходу до безпеки платформ для хмарних та розподілених обчислень /Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases;

NIST SP 800-53 надає список засобів контролю безпеки та приватності для федеральних інформаційних систем і організацій, а також описує процес вибору елементів керування для захисту діяльності організації. Він закладає основу для багатьох стандартів відповідності, включаючи Федеральний закон про модернізацію інформаційної безпеки (FISMA), FedRAMP, NIST Cybersecurity Framework (CSF) і тест безпеки Azure;

Стандарти для категоризації безпеки федеральної інформації та інформаційних систем (2004) / Standards for Security Categorization of Federal Information and Information Systems. Federal Information Processing Standards (FIPS) Publication 199[22];

Циркуляр А-130. Управління інформацією як стратегічним ресурсом. Офіс управління та бюджету США (2016) / Circular A-130, «Managing Information as a Strategic Resource»[23], Office of Management and Budget (OMB).

Федеральна програма управління ризиками та авторизацією, США, 2011 / The Federal Risk and Authorization Management Program, FedRAMP[24];

Настанова щодо вимог безпеки хмарного обчислення, Версія 1, Випуск 4, Департамент оборони США (2022). / DoD Cloud Computing SRG V1R4[25];

Стандарт багаторівневої безпеки хмарних середовищ, Сінгапур / Multi-tiered Cloud Computing Security (MTCS, SPRING SS 584)[26];

Схема сертифікації хмарних сервісів в ЄС / EUCS / ENISA (2020)[27]; Платформа Gaia-X Framework[28], Gaia-X Digital Clearing House (GXDCH)[29], ЄС (2023).

20 PCI SSC Cloud Computing Guidelines. https://www.pcisecuritystandards.org/document_library/?document=dss_cloud_computing_guidelines

21 Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases. https://csrc.nist.gov/publications/detail/nistir/8320/final

22 Standards for Security Categorization of Federal Information and Information Systems. https://csrc.nist.gov/csrc/media/publications/fips/199/final/documents/fips-pub-199-final.pdf

23 Managing Information as a Strategic Resource. https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf

24 Understanding Baselines and Impact Levels in FedRAMP. https://www.fedramp.gov/understanding-baselines-and-impact-levels/

25 U_Cloud_Computing_SRG_V1R4. https://dl.dod.cyber.mil/wp-content/uploads/cloud/zip/U_Cloud_Computing_SRG_V1R4.zip

26 SS584. https://en.wikipedia.org/wiki/SS584

27 EUCS – Cloud Services Scheme. https://ec.europa.eu/newsroom/cipr/redirection/document/76958

28 Gaia-X Framework.https://gaia-x.eu/gaia-x-framework/

29 GXDCH (Gaia-X Digital Clearing House). https://gaia-x.eu/gxdch/

Застосування хмарних сервісів для адміністрування Державного реєстру виборців України

Відповідно до пункту 8 статті 17 Закону України «Про Центральну виборчу комісію»[30] Комісія є розпорядником Державного реєстру виборців (далі – Реєстр), забезпечує його ведення та функціонування відповідно до закону.

Правові та організаційні засади ведення Реєстру визначено Законом України «Про Державний реєстр виборців»[31] (далі – Закон), згідно зі статтею 1 якого Реєстр – це автоматизована інформаційно-комунікаційна система, призначена для зберігання, обробки даних, які містять передбачені Законом відомості, та користування ними, створена для забезпечення державного обліку громадян України, які мають право голосу відповідно до статті 70 Конституції України (далі – виборці).

Основними завданнями Реєстру є ведення персоніфікованого обліку виборців, складання списків виборців для проведення виборів Президента України, народних депутатів України, місцевих виборів, всеукраїнського та місцевих референдумів, а також облік виборчих дільниць, які існують на постійній основі (частина перша статті 2 Закону).

Державний реєстр виборців – автоматизована інформаційно-комунікаційна система, призначена для зберігання, обробки даних (та користування ними, створена для забезпечення державного обліку громадян України, які мають право голосу.

Відповідно до статті 5 Закону, до Реєстру заносяться та в базі даних Реєстру зберігаються встановлені цим Законом відомості про виборця (персональні дані) таких видів: 1) ідентифікаційні персональні дані виборця; 2) персональні дані, які визначають місце та умови голосування виборця; 3) службові персональні дані.

База даних Реєстру, будь-яка її частина, копія бази даних або її частини, персональні дані виборців, що містяться у базі даних Реєстру (далі – персональні дані Реєстру), можуть використовуватися лише для цілей, передбачених статтею 26 Закону України «Про Державний реєстр виборців».

З прийняттям Виборчого кодексу України (№ 396-IX від 19.12.2019)[32] була впроваджена нова функція взаємодії виборців з Реєстром шляхом запровадження в мережі Інтернет електронних сервісів, яку забезпечує розпорядник Реєстру (Служба розпорядника Державного реєстру виборців Секретаріату Центральної виборчої комісії).

Гарантії захисту та безпеки персональних даних виборців у Реєстрі регламентовано статтею 11 Закону. Частиною першою цієї статті на розпорядника Реєстру покладено обов'язок щодо забезпечення захисту Реєстру, у тому числі захист цілісності бази даних Реєстру, його апаратного та програмного забезпечення, достовірності даних Реєстру, його захист від несанкціонованого доступу, незаконного використання, незаконного копіювання, спотворення, знищення даних Реєстру, безпеку персональних даних виборців відповідно до Закону та законів України «Про захист інформації в інформаційно-комунікаційних системах», «Про захист персональних даних», міжнародних договорів у сфері захисту інформації, згода на обов'язковість яких надана Верховною Радою України.

30 Закон України «Про Центральну виборчу комісію». https://zakon.rada.gov.ua/laws/show/1932-15#Text

31 Закон України «Про державний реєстр виборців». https://zakon.rada.gov.ua/laws/show/698-16#Text

32 Виборчий кодекс України. https://zakononline.com.ua/documents/show/482404___691934

Відповідно до статті 9 Закону України «Про захист інформації в інформаційно-комунікаційних системах» відповідальність за забезпечення захисту інформації в системі покладається на власника системи. Власник системи, в якій обробляються державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, утворює службу захисту інформації або призначає осіб, на яких покладається забезпечення захисту інформації та контролю за ним.

Законом України «Про основні засади забезпечення кібербезпеки України»[33] (пункт 1 частини другої статті 4) до об'єктів кіберзахисту віднесено, зокрема, комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси.

Статтею 11 Закону також встановлено що розпорядник Реєстру у взаємодії з Державною службою спеціального зв'язку та захисту інформації України здійснює комплекс заходів для забезпечення технічного захисту персональних та інших даних Реєстру в процесі їх зберігання, обробки та передачі каналами електронних комунікацій відповідно до законодавства України.

Розпорядник Реєстру для забезпечення захисту даних Реєстру встановлює обов'язковий для осіб, яким надається право доступу до бази даних Реєстру, порядок такого доступу з дотриманням вимог цього Закону. Закон містить положення щодо особливостей доступу та використання персональних даних державними органами, яким законом надано право доступу до автоматизованих інформаційних систем, реєстрів та банків даних, держателями (адміністраторами) яких є державні органи (стаття 26).

Державний реєстр виборців має особливості, яких не мають інші публічні електронні реєстри, що пов'язані з організацією і проведенням виборів на закордонних виборчих дільницях. Закон визначає особливості порядку включення до Реєстру, зміни і уточнення персональних даних (усунення неправильностей) у Реєстрі, періодичного поновлення персональних даних щодо осіб, які проживають або перебувають за межами України. Відповідно до частини першої статті 27 Закону, орган ведення Реєстру в Міністерстві закордонних справ України (структурний підрозділ в МЗС) складає попередні списки виборців, які проживають або перебувають за межами України, для кожної закордонної виборчої дільниці. Попередній список виборців для закордонної виборчої дільниці передається відповідній дільничній виборчій комісії в електронному вигляді (частина шоста статті 27). Так само у електронному вигляді передаються уточнені списки виборців для закордонних виборчих дільниць (частина сьома статті 28).

Концепція створення Єдиної автоматизованої інформаційно-аналітичної системи Центральної виборчої комісії (ЄІАС ЦВК)[34] основними принципами її побудови визнає забезпечення гнучкості та інформаційної повноти за рахунок інтеграції, регламентованої доступності функцій та даних для конкретних компонентів, користувачів ЄІАС ЦВК.

Компоненти ЄІАС ЦВК мають функціонувати за єдиними стандартами та технологіями, що забезпечують перенесення даних, належний рівень захисту інформації та кібербезпеки інформаційних систем Комісії, ефективне управління обчислювальними ресурсами, багаторазове використання програмних компонентів та сервісів. Усі компоненти ЄІАС ЦВК повинні функціонувати відповідно до положень законодавства України. Під час створення ЄІАС ЦВК необхідно передбачити можливість масштабування, модернізації, розширення функціональних можливостей її компонентів, зокрема в разі внесення змін до законодавства, без суттєвих змін у прикладному програмному забезпеченні. **Для забезпечення доступності та надійності, Концепцією передбачається повне резервування як програмних, так і апаратних складових усіх інформаційних ресурсів.**

33 Закон України «Про основні засади забезпечення кібербезпеки України». https://zakon.rada.gov.ua/laws/show/2163-19#Text

34 Постанова Центральної виборчої комісії «Про схвалення Концепції створення Єдиної автоматизованої інформаційно-аналітичної системи Центральної виборчої комісії». https://zakon.rada.gov.ua/laws/show/v0447359-21#Text

Постановою ЦВК від 24 лютого 2022 року № 61 «Про тимчасове припинення функціонування автоматизованої інформаційно-комунікаційної системи «Державний реєстр виборців» на час дії воєнного стану»[35] тимчасово припинено функціонування автоматизованої інформаційно-комунікаційної системи «Державний реєстр виборців», припинено ведення Державного реєстру виборців на час дії воєнного стану. Службі розпорядника Державного реєстру виборців Секретаріату Центральної виборчої комісії наказано невідкладно здійснити заходи, спрямовані на захист цілісності бази даних Державного реєстру виборців, його апаратного та програмного забезпечення.

ЦВК повинна мати можливість відновлення після можливого збою своїх серверів впродовж прийнятного часу. Резервне копіювання є важливою частиною операцій із захисту інформації та кібербезпеки. Розміщення резервних копій бази даних Реєстру у захищеній хмарній інфраструктурі є одним із можливих способів фізичної сегрегації для гарантування безпеки виборчої архітектури. Хмарні технології можуть застосовуватися для розміщення відкритих систем ЄІАС ЦВК, таких як підсистема веб-відображення результатів голосування, для використання програмного забезпечення, розміщеного на серверах хмарного постачальника за моделлю (SaaS) тощо. Цими рішенням варто скористатися не лише з огляду на поточні ризики знищення, порушення цілісності, конфіденційності чи втрати доступу до державних інформаційних ресурсів в ході триваючого збройного конфлікту, а визнати це системним рішенням з побудови більш стійкої інформаційної інфраструктури.

35 Постанова Центральної виборчої комісії «Про тимчасове припинення функціонування автоматизованої інформаційно-комунікаційної системи «Державний реєстр виборців» на час дії воєнного стану». https://zakon.rada.gov.ua/laws/show/v0061359-22#Text

3. Короткий огляд інституційного і регуляторного розвитку хмарної інфраструктури в Європейському Союзі

Для Європейського Союзу дані є ключовим пріоритетом для економічного зростання, будь то для полегшення персоналізованої медицини або автономних транспортних засобів. Між 2018 та 2025 роками прогнозується, що вартість економіки даних в Європі майже потроїться, з € 301 мільярдів до € 829 мільярдів, а кількість фахівців з даних майже подвоїться. Оскільки розмір даних передбачається збільшитися у п›ять разів протягом цього періоду, хмарні сервіси є ключовими для споживання економічної вигоди від зберігання та циркуляції даних.

Хмарна стратегія Європейської Комісії[36]

Цифрова стратегія Європейської Комісії передбачає перехід до *«цифрового управління керованого даними та орієнтованого на користувачів»*. Одним з ключових факторів цієї трансформації є хмарні обчислення. Цей новий підхід надання IT-послуг дозволяє використовувати IT-ресурси на вимогу та зменшує необхідність інвестування в IT-інфраструктуру.

Другим фактором є новий спосіб розробки інформаційних систем на основі хмарних IT-сервісів, що дозволяє зосередитися на цінності бізнесу та зменшити складність інформаційної системи. Разом ці дві зміни забезпечують трансформаційні зміни в IT-сфері, які підтримують трансформацію бізнес-процесів та забезпечують більш ефективне управління даними та ресурсами.

Європейська Комісія активно підтримувала хмарні обчислення як для компаній, так і для державних адміністрацій, після того, як була прийнята перша Європейська стратегія хмарних обчислень у 2012 році. Згідно з європейською політикою щодо хмарних технологій у державних органах, DIGIT започаткувала експерименти з хмарними обчисленнями в інституціях та агенціях ЄС і об'єднала досвід у вичерпний перелік отриманих уроків.

Цей досвід підтвердив трансформаційний потенціал хмарних обчислень, проте також показав, що корпоративне управління та управління безпекою повинні отримати особливу увагу, щоб уникнути небажаного впливу ризиків у сфері витрат та безпеки інформації. Отже, хоча хмарні технології мають великий потенціал для трансформації бізнес-процесів та підвищення ефективності управління даними, важливо забезпечити високий рівень безпеки та ефективного управління, щоб уникнути можливих ризиків та негативних наслідків.

36 European Commission Cloud Strategy. https://commission.europa.eu/publications/european-commission-cloud-strategy_en

На основі цього Європейська Комісія сформувала візію хмарних обчислень:

«Насамперед хмарні технології з пропозицією безпечного гібридного багатохмарного сервісу»

Хмарні технології – це майбутнє IT-індустрії, яке пропонує безліч можливостей для компаній та держав. А серед них найбільш перспективною є безпечний гібридний багатохмарний сервіс, який поєднує в собі найкращі можливості кількох хмарних сервісів. За допомогою цієї технології компанії можуть забезпечити високий рівень безпеки та ефективного управління даними, одночасно маючи можливість використовувати різні хмарні сервіси залежно від потреб бізнесу. Це підвищує конкурентоспроможність компаній та дозволяє їм бути готовими до змін, які можуть виникнути у майбутньому.

«Насамперед хмарні технології» (Cloud First) означає, що системи мають бути створені таким чином, щоб вони могли скористатися перевагами хмарних моделей доставки, які існують як на місці, так і в загальнодоступній хмарі. **Вибір архітектури, особливо локальної та/або публічної хмари, залежить від переваг, обмежень і ризиків для конкретної системи.** Тож це не означає, що всі системи мають перейти до публічної хмари.

Європейська Комісія визначила такі принципи:

- **безпечність** є найважливішим принципом, на якому будується пропозиція. Інформаційні та технологічні ризики повинні бути виявлені та вирішені згідно з класифікацією даних та зобов›язаннями Європейської Комісії щодо захисту даних;
- **гібридність** передбачає використання як послуг публічних хмар, так і локальної приватної хмари, що керується самою Європейською Комісією. Це дозволить відповідати на потреби і вимоги різних відділів та програм;
- **багатохмарність** полягає у тому, що Європейська Комісія не буде прив›язана до одного хмарного постачальника та джерела, а використовуватиме різні постачальники, які найкраще підходять для певних запитів;
- пропозиція повинна бути **енергоефективною** та відповідати політиці ЄС зменшення викидів вуглецю. Державні закупівлі мають бути зорієнтовані на покращення екологічних показників.

Для реалізації цього бачення передбачено зміни в кількох ключових сферах:

У сфері *управління IT* Європейська Комісія в контексті пакету заходів щодо управління, ухваленого в листопаді 2018 року, перегляне процеси управління життєвим циклом інформаційних систем і переконається, що вони придатні для виконання всіх аспектів хмарних обчислень. Крім того, будуть запроваджені необхідні механізми для забезпечення того, щоб дорожні карти модернізації, необхідні в контексті Цифрової стратегії Європейської Комісії, узгоджувалися з принципом «насамперед хмарні технології».

Управління ризиками, пов'язаними з хмарою, підтримуватиметься новим інструментом GovSec, який пропонує практичну підтримку управління ризиками для хмарних систем. Інструмент забезпечить практичний і загальний підхід до управління хмарними ризиками, заощаджуючи дорогоцінний час на етапі обов'язкової оцінки ризиків проектів, а також забезпечуючи спільну базову лінію для Європейської Комісії, інституцій та агенцій.

DIGIT продовжуватиме працювати як міжінституційний хмарний брокер, щоб дати Європейській Комісії та зацікавленим Європейським установам і агенціям можливість ефективно та безпечно замовляти хмарні послуги від широкого кола постачальників хмарних послуг, зменшити ризик блокування

постачальника, полегшити моніторинг і прогнозування витрат і надати рекомендації. Для Європейської Комісії *Cloud Broker* також надаватиме базові хмарні послуги та забезпечуватиме загальну базову лінію безпеки та захисту даних у всіх хмарах.

У сфері *цифрових рішень* Європейська Комісія надаватиме перевагу генеруванню загальних або стандартних рішень на ринку хмарних бізнес-додатків (SaaS).

У сфері *багатохмарності* Європейська Комісія перетворить існуючі сервіси, фреймворки та технічні платформи на багатохмарні сервіси комплексної платформи.

У сфері *екосистеми даних* Європейська Комісія перетвориться на організацію, керовану даними, створивши екосистему даних для збору, керування, зберігання, захисту, розробки, доступу, використання, повторного використання, споживання, аналізу, розповсюдження та обміну даними.

У сфері *цифрового робочого місця DIGIT* використовуватиме гібридну хмарну платформу *SaaS*, щоб надати Європейській Комісії цифрове робоче середовище, яке дозволить користувачам працювати та співпрацювати будь-де та будь-коли з будь-якого корпоративного пристрою.

У сфері *цифрових інфраструктур DIGIT* надаватиме послуги гібридної хмари Європейській Комісії та зацікавленим установам і агентствам. Для досягнення цієї мети компанія створить службу архітектури гібридного хмарного рішення та перетворить свої послуги центру обробки даних у гібридні хмарні служби, створені на основі публічної та локальної приватної хмарної інфраструктури.

У сфері *хмарних служб безпеки* DIGIT надаватиме Європейській Комісії хмарні послуги безпеки на всіх етапах життєвого циклу всіх типів використання хмарних послуг.

***

Хмарні обчислення є ключовим інструментом для посилення *цифрового суверенітету Європи*, як це передбачено в Стратегії даних Європейської комісії, Цифровій стратегії, Промисловій стратегії, Плані відновлення ЄС та Європейському рамковому документі про інтероперабельність. Європейська Комісія підтримала створення Європейського альянсу щодо промислових даних, мережевих технологій та хмарних сервісів[37], який включає розробку декількох напрямків, пов'язаних з ключовими цілями політики ЄС. У грудні 2020 року Європейська комісія запустила Європейську Хмарну Федерацію[38] для розвитку європейської хмарної екосистеми. Федерація включає європейських надавачів хмарних послуг та має на меті просування розробки безпечних та інтероперабельних хмарних послуг в Європі.

Gaia-X (Gaia-X European Association for Data and Cloud)[39] – це проект, який має на меті розробити спільний фреймворк для європейської інфраструктури даних та створити консорціум між публічними та приватними компаніями. В ньому беруть участь понад 300 учасників, серед яких багато європейських та міжнародних компаній. GAIA-X має на меті визначити мінімальні технічні вимоги та послуги, необхідні для роботи розподіленої екосистеми GAIA-X, яка заснована на принципах «безпека за дизайном» і «приватність за дизайном». Асоціація бачить свій «GXDCH» (Gaia-X Digital Clearing House)[40], як ефективний інструмент, що забезпечить достатньо великий обсяг ринку, щоб зробити Gaia-X стандартом інфраструктури даних «де-факто».

37 European Alliance for Industrial Data, Edge and Cloud. https://digital-strategy.ec.europa.eu/en/policies/cloud-alliance

38 European cloud federation promoting development european cloud ecosystem.

39 Gaia-x https://gaia-x.eu/

40 Market-X Conference & Expo: Gaia-X Digital Clearing House (GXDCH) a success for the industry. https://gaia-x.eu/news/latest-news/market-x-conference-expo-gaia-x-digital-clearing-house-gxdch-a-success-for-the-industry/

Платформа Gaia-X Framework[41] описує функціональні специфікації, технічні вимоги та активи програмного забезпечення, необхідні для сумісності з Gaia-X. GXDCH пропонує універсальне рішення для перевірки дотримання правил Gaia-X автоматизованим способом. GXDCH — це мережа вузлів виконання для компонентів відповідності, що підтримує відкриту, прозору та безпечну федеративну цифрову екосистему. У березні 2023 р. було анонсовано[42] перші два вузли GXDCH: Aruba та T-systems.

Європейський Союз (ЄС) розробив кілька політик та ініціатив, що мають безпосереднє відношення до розвитку публічних хмарних сервісів:

Стратегія даних Європи[43]: У лютому 2020 року Європейська комісія прийняла Стратегію даних Європи, яка включає кілька заходів для сприяння використанню хмарних обчислень та інших цифрових технологій в Європі. Ці заходи включають сприяння використанню безпечних та інтероперабельних хмарних сервісів, підтримку розвитку європейського простору даних та просування використання штучного інтелекту. Європейський акт про управління даними (DGA, 2022)[44] сприяє обміну даними між секторами та країнами ЄС, щоб використовувати потенціал даних на користь громадян і підприємств ЄС. Мета полягає в тому, щоб створити єдиний європейський простір даних.

Акт про цифрові послуги[45]: У грудні 2020 року Європейська комісія запропонувала Акт про цифрові послуги (DSA), який включає нові правила для онлайн-платформ, включаючи постачальників хмарних сервісів. Запропонований регуляторний акт має на меті підвищити прозорість та відповідальність онлайн-платформ, просувати інновації та конкуренцію в цифровому секторі.

EU Cloud Rulebook[46] має стати набором правил для хмарних сервісів, який забезпечуватиме єдину європейську рамку правил, прозорість відносно їх відповідності та найкращі практики для використання хмарних технологій в Європі, зокрема встановити загальноєвропейські правила для хмарних обчислень, включаючи такі області, як безпека даних, конфіденційність даних, можливість перенесення даних (data portability) та енергоефективність.

Кодекс поведінки щодо хмарних сервісів у ЄС: У лютому 2021 року Асоціація постачальників інфраструктури хмарних сервісів Європи (CISPE) запустила Кодекс поведінки щодо хмарних сервісів, який надає набір рекомендацій постачальникам хмарних сервісів для забезпечення відповідності правилам захисту персональних даних ЄС (GDPR). Кодекс має на меті сприяти довірі та прозорості в хмарних сервісах та забезпечити відповідність хмарних сервісів правилам ЄС щодо захисту даних.

Схема сертифікації хмарних сервісів ЄС ***(EUCS)***[47]

Схема EUCS створена в рамках Закону про кібербезпеку (CSA)[48]. Як передбачено у статті 48(2) Закону, у 2021 році Агентство Європейського Союзу з кібербезпеки (ENISA) провело публічні консультації для зацікавлених сторін щодо проекту Схеми сертифікації кібербезпеки Європейського Союзу щодо хмарних послуг (EUCS). Метою проекту є забезпечення вдосконалення умов внутрішнього ринку Союзу для хмарних послуг шляхом посилення та оптимізації їхніх гарантій кібербезпеки.

41 Gaia-X Framework. https://gaia-x.eu/gaia-x-framework/

42 Market-X Conference & Expo: Gaia-X Digital Clearing House (GXDCH) a success for the industry. https://gaia-x.eu/news/latest-news/market-x-conference-expo-gaia-x-digital-clearing-house-gxdch-a-success-for-the-industry/

43 European data strategy. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en

44 The European Data Governance Act (DGA). https://www.european-data-governance-act.com/

45 Proposal regulation european parliament and council digital services act.

46 Position paper - EU Cloud Rulebook and related cloud initiatives. https://www.amchameu.eu/position-papers/eu-cloud-rulebook-and-related-cloud-initiatives

47 EU Cloud Certification Scheme. https://ec.europa.eu/newsroom/cipr/items/713799/en

48 Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32019R0881

Проект спрямований на гармонізацію безпеки хмарних сервісів з правилами ЄС, міжнародними стандартами та промисловою практикою, а також з існуючими сертифікатами в країнах-членах ЄС. Проект має на меті вирішити проблеми, що виникають при сертифікації хмарних послуг, визначаючи базову лінію безпеки для кожного з трьох рівнів надійності. Сертифікаційна схема ***EUCS (2021)***[49] **є горизонтальною технологічною схемою та дозволяє перехід від поточних національних схем до загальноєвропейської**. Схема охоплює три рівні гарантій – «Базовий», «Значний» і «Високий» та надає трирічну сертифікацію, яку можна поновити. Крім того, проект включає **вимоги щодо прозорості, наприклад, щодо місця обробки та зберігання даних. Вбачається доцільним для України розпочати будувати національну схему сертифікації хмарних послуг одразу на підставі EUCS**.

Загальний регламент про захист персональних даних (GDPR)[50]. Однією з ключових областей фокусу для ЄС є безпека даних. Загальний регламент про захист персональних даних, який набрав чинності у травні 2018 року, встановлює строгі правила для захисту персональних даних, включаючи дані, які зберігаються та обробляються у хмарі. Наразі GDPR є взірцем для побудови систем захисту персональних даних також в інших країнах. GDPR є повністю технологічно нейтральним і пропагує застосування принципу контрольованості (accountability principle), за яким організація-контролер даних відповідальна за вжиття таких організаційних й технічних заходів, що дозволять дотримуватися положень GDPR при обробці персональних даних. Важливо підкреслити, GDPR застосовується до усіх організацій в ЄС, а також має екстериторіальну дію. Тому вимоги GDPR застосовуються до всіх організацій поза межами ЄС, якщо такі організації цілеспрямовано пропонують послуги і обробляють персональні дані осіб в ЄС незалежно від їх громадянства. **Із самого початку потенційного співробітництва надавачам хмарних послуг потрібно дотримуватися стандартів GDPR, зважаючи на наступне:**

- якщо надавач хмарних послуг в ЄС, то GDPR є для нього обов'язковим в силу положень цього регламенту,
- якщо надавач хмарних послуг поза межами ЄС, відповідність GDPR, по факту, є також обов'язковою, тому що з організаційної і технічної точок зору потрібна повна інтегрованість серверів такого провайдера із системами в ЄС, що дозволить швидко і безперешкодно передавати персональні дані, в разі потреби,
- окремо потрібно зазначити про те, що наразі українське законодавство із захисту персональних даних реформується, за основу для реформування взято саме GDPR. Тому в найближчому майбутньому до обробки персональних даних українців будуть застосовуватися організаційні й технічні норми рівня GDPR.

NIS2[51] є другою версією Директиви ЄС щодо мереж та інформаційних систем, яка має на меті забезпечення високого рівня безпеки мереж та інформаційних систем в усьому ЄС. Вона набула чинності 16 січня 2023 року, і країни-члени мають 21 місяць, до 17 жовтня 2024 року, щоб внести її положення до національного законодавства. Вона застосовується до операторів основних послуг (OES) та постачальників цифрових послуг (DSP), включаючи надавачів хмарних послуг (CSP). Глобальні та європейські надавачі хмарних послуг знаходяться в області дії NIS2 і, отже, повинні виконувати вимоги NIS2.

49 EUCS – Cloud Services Scheme.https://ec.europa.eu/newsroom/cipr/redirection/document/76958

50 General Data Protection Regulation. https://gdpr-info.eu/

51 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance).

Імплементація NIS2 надає Україні такі ключові переваги:

1) це дозволить ділитися передовими практиками та експертизою на українському ринку кібербезпеки критичної інфраструктури;

2) це дозволить надавачам хмарних послуг, які працюють в ЄС, отримати доступ до українського ринку з меншими перешкодами, оскільки вони вже відповідають вимогам NIS2 (в порівнянні з будь-яким іншим потенційним законодавством, що відрізняється від NIS2);

3) це дозволить українським органам та CSIRTs краще отримувати доступ до європейської кібербезпекової екосистеми, оскільки законодавчі та оперативні рамки по обидві сторони будуть сумісними, що дозволить «спілкуватися однією мовою» з колегами з ЄС.

Директива CER[52] була введена в ЄС разом з директивою NIS2. При розробці політики та законодавства щодо фізичної безпеки необхідно розуміти особливості цифрових інфраструктурних провайдерів, таких як надавачі хмарних послуг та оператори центрів обробки даних. Організації, що потрапляють в сферу дії директиви CER, повинні застосовувати комплексний підхід, в якому вимоги щодо кібербезпеки також охоплюють фізичну безпеку.

Європейська рамка інтероперабельності (EIF)[53] надає конкретні рекомендації щодо налагодження інтероперабельності цифрових публічних сервісів. EIF надає 47 рекомендацій, 12 принципів, які повинні керувати політикою в цілому, шари взаємодії, які представляють різні аспекти взаємодії, які повинні бути враховані при проектуванні європейських публічних сервісів; та концептуальну модель, яка має на меті проектування та надання інтегрованих публічних сервісів. Для України існує приваблива перспектива застосувати Європейську рамку інтероперабельності для інтеграції своїх електронних публічних послуг в загальноєвропейську екосистему за допомогою хмарних технологій.

Імплементація вищезазначених актів права Європейського Союзу потребує аналізу та виявлення невідповідностей, які необхідно усунути до початку та в рамках переговорного процесу щодо вступу України до Європейського Союзу, про що зокрема, зазначається у Порядку проведення первинної оцінки стану імплементації актів права Європейського Союзу (acquis ЄС), затвердженому постановою Кабінету Міністрів України від 28 лютого 2023 р. № 189.[54]

52 Directive (Eu) 2022/2557 Of The European Parliament And Of The Council. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557

53 The European Interoperability Framework in detail. https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail

54 Постанова Кабінету Міністрів України «Про затвердження Порядку проведення первинної оцінки стану імплементації актів права Європейського Союзу». https://zakon.rada.gov.ua/laws/show/189-2023-%D0%BF#Text

4. Міжнародний досвід і світові практики

Національна хмара Естонії

Riigipilv[55] — це хмарне середовище, кероване державою, яке дає змогу пропонувати державному сектору централізовані хмарні рішення та супутні послуги. За адміністрування національної хмари на цей час відповідає Державний центр інформаційно-комунікаційних технологій[56]. До лютого 2022 року адміністратором хмари був Державний фонд інфокомунікацій (PIKC). У 2015 року Рада PIKC затвердила план розвитку на 2016-2020 роки, в якому було поставлено завдання реалізувати розроблену Міністерством економіки та зв'язку Естонії концепцію «Національної хмари»[57]. Далі відбулася підготовка та проведення концесійних закупівель для впровадження пілотного проекту державних хмарних сервісів відповідно до плану заходів, представленого на розгляд ради та затвердженого нею. Для створення та розгортання платформи через державні закупівлі було залучено консорціум, до складу якого входять Cybernetica AS, Dell EMC, Ericsson Eesti AS, OpenNode OÜ і Telia Eesti AS.

Метою національної хмари є зробити державні послуги стійкішими, швидшими та зручнішими, відповідаючи високим вимогам безпеки та потребам цифрового суспільства Естонії, а також забезпечити більш економічне управління державними установами в довгостроковій перспективі.

Окрім державного сектору, користувачами хмари є органи місцевого самоврядування, постачальники критично важливих послуг (оператори критичної інфраструктури), приватні компанії, що надають IT-послуги державі, і постачальники медичних послуг. Користувачі національної хмари можуть швидко збільшити або зменшити обсяг використовуваних ресурсів відповідно до своїх потреб і замовити або скасувати додаткові послуги.

Естонська національна хмара — це гібридна хмара, розроблена для підтримки безперервності послуг інформаційного суспільства Естонії, яка включає приватну (індивідуальну) хмару, що надає послуги державним установам, публічні (колективні) хмари, якими керує приватний сектор, і посольства даних, розташовані в інших країнах. Каталог хмарних послуг постійно поповнюється послугами типу IaaS, PaaS і SaaS.

Відносини з партнерами по консорціуму є договірними, що визначає як повноваження, так і відповідальність. Крім того, права доступу партнерів сегментовані таким чином, що права розподіляються відповідно до сфери діяльності адміністратора. Це означає, що адміністратори мережевих пристроїв можуть отримати доступ до мережевих пристроїв, адміністратори сервісного рівня можуть отримати доступ до сервісних серверів і так далі. Це зводить до мінімуму небезпеки надання повних прав.

Національна хмара відповідає найвищому рівню безпеки (*ISKE H*), встановленому в естонському національному стандарті безпеки інформаційних систем, який повинен забезпечувати конфіденційність і цілісність IT-інфраструктури та інформації. Крім того, абонент також може вибрати з каталогу послуг послуги з іншим рівнем безпеки, ніж *ISKE H*.

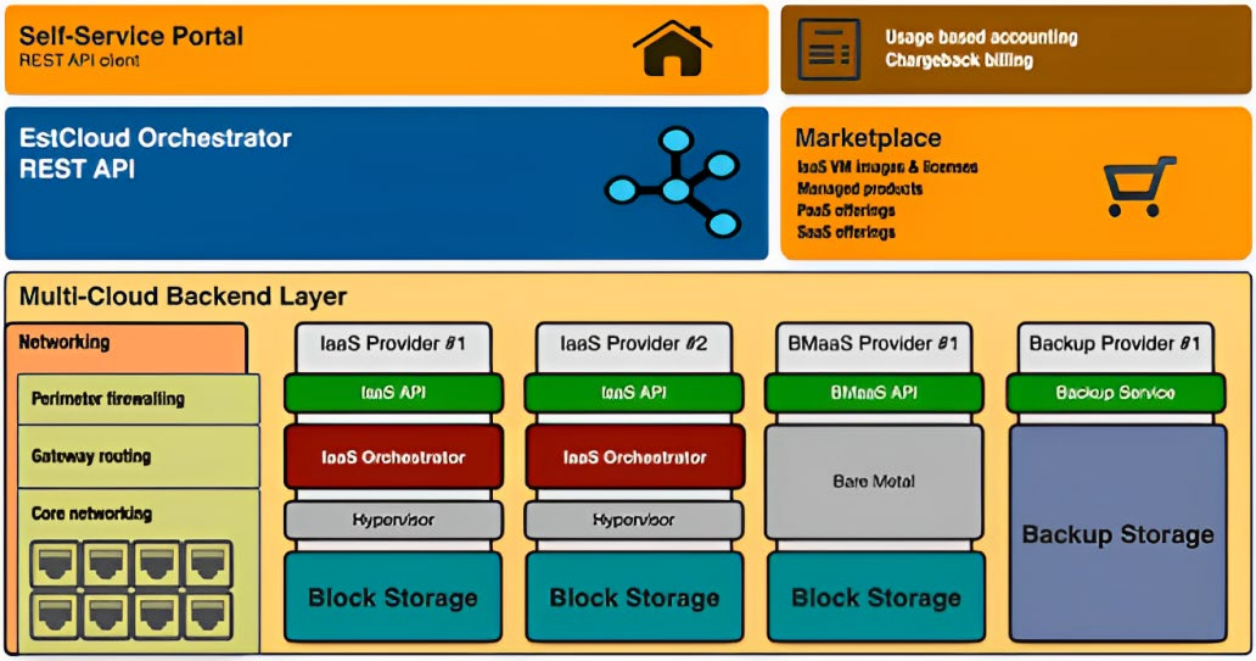
55 Estonian Government Cloud. https://www.riigipilv.ee/en

56 Estonian IT Centre. https://www.rit.ee/

57 Eesti riigipilve kontseptsioon. https://riigipilv.ee/files/Eesti_riigipilve_kontseptsioon.pdf

Архітектура національної хмари Естонії

Національна хмара технічно побудована за модульним принципом – використовується стандартне апаратне забезпечення, а програмні компоненти, по можливості, мають відкритий код і мають загальнодоступний вихідний код.



Платформа управління всіма хмарними послугами – це середовище самообслуговування Waldur[58], яке включає інструменти для керування ресурсами в усіх місцях хмари, опцію інтерфейсу REST API[59], систему виставлення рахунків, каталог послуг і портал для клієнтів, через який здійснюється спілкування з клієнтами. Усі функції хмари стану контролюються API. Середовище самообслуговування — це графічний інтерфейс API для використання людиною.

Румунська урядова хмара

У червні 2022 року Уряд Румунії ухвалив Надзвичайну Постанову про впровадження урядової хмарної платформи[60] (далі – Постанова). Серед чинників, що вплинули на прийняття Постанови зазначається надзвичайна ситуація, спричинена збройним конфліктом на території України, та нагальна потреба у підвищенні можливостей стійкості IT-систем і мереж румунської держави, у тому числі через призму необхідності забезпечення безпеки персональних даних громадян Румунії.

Постанова встановлює загальну структуру для створення, управління та розвитку на національному рівні гібридної хмарної інфраструктури, яка називається «Платформа». Органами, відповідальними за реалізацію Платформи, є Міністерство досліджень, інновацій та цифровізації (MCID) та Агентство з цифровізації (ADR) у співпраці з Державною службою спеціальних комунікацій (STS) та Державною інформаційною службою (SRI).

Розпорядженням Уряду Румунії у січні 2023 року було затверджено Інструкцію з управління урядовою хмарною платформою[61], що має на меті:

58 Waldur MasterMind. https://github.com/opennode/waldur-mastermind

59 Waldur Documentation. API. https://opennode.atlassian.net/wiki/spaces/WD/pages/22976823/API

60 Ordonanță De Urgență Nr. 89 Din 27 Iunie 2022. https://legislatie.just.ro/Public/DetaliiDocumentAfis/256832

61 Hotărârea nr. 112/2023 privind aprobarea Ghidului de guvernanță a platformei de cloud guvernamental. https://lege5.ro/gratuit/geztgmzrgu3di/hotararea-nr-112-2023-privind-aprobarea-ghidului-de-guvernanta-a-platformei-de-cloud-guvernamental

- встановлення стандартів, правил і зобов'язань, необхідних для операційної, процедурної та технічної діяльності з організації та експлуатації IT-інфраструктури та хмарних послуг;
- визначення структури управління та зберігання даних на Платформі та встановлення категорій даних, що обробляються та/або розміщуються на Платформі, у тому числі в державному приватному (індивідуальному) хмарному компоненті;
- план міграції та інтеграції до Платформи IT-додатків та електронних публічних послуг установ і органів державної влади, а також перелік органів влади та державних установ, чиї IT-системи та електронні публічні послуги мігрують на Платформу;
- загальні критерії забезпечення конфіденційності, безпеки, сумісності, адаптації до технічних і семантичних стандартів, відповідно продуктивності додатків і хмарних послуг, таких як IaaS, PaaS, SaaS, розміщених на Платформі, включаючи методологічні правила щодо журналювання подій та доступ органів влади та державних установ до даних, розміщених на Платформі.

Структура Платформи

Платформа складається з двох компонентів: (а) компонент приватної хмари, який називається «приватна (індивідуальна) урядова хмара», і (б) сертифіковані загальнодоступні ресурси та послуги з інших публічних або приватних хмар («неприватна (колективна) урядова хмара»).

Постанова визначає приватну (індивідуальну) хмару як спосіб організації ресурсів системи хмарних обчислень, у якій послуги використовуються єдиним користувачем хмари, а ресурси контролюються саме цим користувачем. З іншого боку, публічна (колективна) хмара визначається як спосіб організації ресурсів системи хмарних обчислень, у якій послуги потенційно доступні будь-якому користувачу хмари, а ресурси контролюються постачальником хмарних послуг. Нарешті, гібридна хмара охоплює як публічні, так і приватні хмари як спосіб організації ресурсів хмарної системи з використанням принаймні двох різних типів хмарних обчислень.

Cloud First

Відповідно до Постанови, публічні організації, чиї системи мають право мігрувати в хмарні служби, повинні відповідати політиці «насамперед хмарні технології». За цим принципом хмарні технології отримують пріоритет перед усіма іншими технологіями, незалежно від того, чи це новий проект, що включає IT та IT-рішення, комунікаційні рішення або технологічну модернізацію існуючої IT-системи.

Особливі вимоги

Як приватні, так і неприватні державні хмари повинні мати у своїй структурі такі технічні компоненти: (i) базову хмарну інфраструктуру; (ii) Інфраструктура як послуга (IaaS); (iii) Платформа як послуга (PaaS); (iv) Програмне забезпечення як послуга (SaaS).

Приватна (індивідуальна) урядова хмара:

- Вищезазначені компоненти, включені до приватної урядової хмари, є власністю держави, перебувають в оперативному управлінні Державної служби спеціальних комунікацій або Агентства з цифровізації. Якщо набуття у власність компонентів неможливе, забезпечуватиметься набуття прав користування.
- Адміністратори послуг IaaS, PaaS і SaaS, а також адміністратори кібербезпеки повинні забезпечити реєстрацію подій і доступ до даних, розміщених у приватній урядовій хмарі, для періодичного аудиту відповідності.

Неприватна (колективна) урядова хмара:

- Інфраструктури хмарних обчислень із неприватної урядової хмари мають бути впроваджені, щоб забезпечити низку можливостей, спеціально наданих Постановою.
- Кожна хмарна послуга повинна забезпечуватися щонайменше двома центрами обробки даних, щоб сприяти стійкості хмарних послуг.
- Центри обробки даних можуть розміщувати приватні, публічні або гібридні хмарні послуги.

Ринок («маркетплейс») платформи

Постанова вводить поняття «ринок», який являє собою каталог хмарних програм і послуг, доступних на Платформі, які також можуть розроблятися приватними компаніями, і до яких можуть отримати доступ державні органи та установи, розміщені в Платформі. Регулятором ринку є Агентство з цифровізації. До програм, доступних на Платформі, можна отримати доступ після укладення угоди між постачальниками хмарних послуг і розміщеними організаціями (наприклад, державними органами та установами), які купують ці послуги.

Захист даних

Постанова також містить положення щодо обробки персональних даних, згідно з якими (i) усі дії з обробки повинні виконуватися відповідно до положень GDPR та законодавства Румунії, і (ii) громадяни будуть негайно інформуватися про доступ до їхніх даних органами державної влади.

Фінансування Платформи

Для впровадження Платформи, а також IaaS, PaaS, SaaS, поряд із забезпеченням компонентів кібербезпеки та міграції бази даних, державні органи – Агентство з цифровізації (ADR), Державна служба спеціальних комунікацій (STS) та Державна інформаційна служба (SRI) – організовуватимуть процедури державних закупівель відповідно до чинного румунського законодавства про державні закупівлі.

Хмарна рамкова програма Великої Британії

Урядовий хмарний проект Великої Британії, відомий як G-Cloud, був запущений у 2012 році і вже досяг своєї 13-ої річниці - «G-Cloud 13».

До цього часу відбулося 12 публічних оголошень-запрошень для укладання контрактів, під час яких постачальники мали можливість перелічити свої послуги в G-Cloud. Рамкова угода G-Cloud не має обмежень, тому якщо заявка відповідає вимогам, необмежена кількість постачальників може приєднатися до рамкової угоди. Рамкова угода G-Cloud поділена на категорії (Лоти), і постачальники можуть подати заявку на один, два або три Лоти, залежно від того, які рішення вони пропонують для публічного сектору.

- Лот 1: Хмарний хостинг (IaaS та PaaS)

Цей Лот охоплює хмарні платформи та інфраструктурні сервіси, які дозволяють покупцям розгортати, керувати та запускати програмне забезпечення, а також надавати та використовувати ресурси для обчислень, зберігання або мережі.

- Лот 2: Хмарне програмне забезпечення (SaaS)

Цей Лот призначений для додатків, до яких зазвичай звертаються через публічну або приватну мережу, наприклад, Інтернет, та які знаходяться в хмарі.

- Лот 3: Підтримка хмари

Цей Лот передбачає послуги, які допомагають покупцям налаштовувати та підтримувати їхнє хмарне програмне забезпечення або хостинг-сервіси.

- Лот 4: Хмарна міграція

У 2022 році, у G-Cloud 13, з›явився абсолютно новий Лот 4 для проектів хмарної міграції великого масштабу. Це включає планування, налаштування, хмарні міграційні послуги, послуги забезпечення безпеки, постійну підтримку та інше. Постачальники, що входять до цього Лоту, мають надавати всі ці послуги, та проходитимуть відбір, щоб до нього потрапити, адже кількість місць для участі обмежена.

G-Cloud складається з низки рамкових угод із постачальниками хмарних послуг, та списку їхніх послуг на цифровому ринку (Digital Marketplace). Це дозволяє організаціям публічного сектору порівнювати та придбавати ці послуги, не проводячи власний повний процес огляду. Включення у Digital Marketplace передбачає самооцінку відповідності вимогам, після чого Урядова цифрова служба (Government Digital Service) може на власний розсуд здійснювати перевірку.

Процес призначення в G-Cloud був спрощений у 2014 році, щоб зменшити час та витрати для уряду Великої Британії, та класифікаційна схема безпеки уряду була спрощена з шести до трьох рівнів: «Службова», «Таємна» та «Цілком таємна». Рівні сертифікації G-Cloud більше не виражаються в рівнях впливу (Impact Level), які досі застосовуються у США (див. нижче).

Замість централізованої оцінки хмарних послуг, яка надавалася раніше, новий процес вимагає, щоб надавачі хмарних послуг самостійно оцінювали свою відповідність та надавали докази, що підтверджують виконання 14 принципів-вимог[62] з безпеки хмар G-Cloud.

Оцінка з використанням принципів хмарної безпеки не замінює необхідності виконувати оцінку впливу на захист даних (DPIA)[63]. DPIA – це процес оцінки ризиків, пов›язаних з обробкою персональних даних, який повинен бути виконаний згідно із Загальним регламентом захисту даних (GDPR) ЄС, який встиг стати частиною законодавства Великої Британії до виходу з ЄС. Оцінка з використанням принципів хмарної безпеки – це важлива складова в оцінці ризиків, пов›язаних з використанням хмарних послуг, проте DPIA необхідно виконувати окремо, оскільки вона охоплює ширший спектр ризиків, пов›язаних з обробкою персональних даних.

В екосистемі хмарної індустрії Великої Британії також існують брокери хмарних послуг (постачальники, які агрегують декілька різних хмарних послуг для надання їх клієнту уніфікованої пропозиції) та хмарні біржі (постачальники, які пропонують безпосереднє з›єднання між кількома хмарними платформами, дозволяючи їхнім клієнтам отримувати доступ до та переносити свої дані між окремими хмарними платформами, не передавши їх через Інтернет). У контексті гібридної моделі розгортання, «розрив хмар» (*cloudbursting*) стає все більш поширеним, коли клієнти переносять певні процеси, що виконуються власними силами, до публічних хмарних сервісів, щоб забезпечити більшу ємність.

Національна хмарна модель Сінгапуру

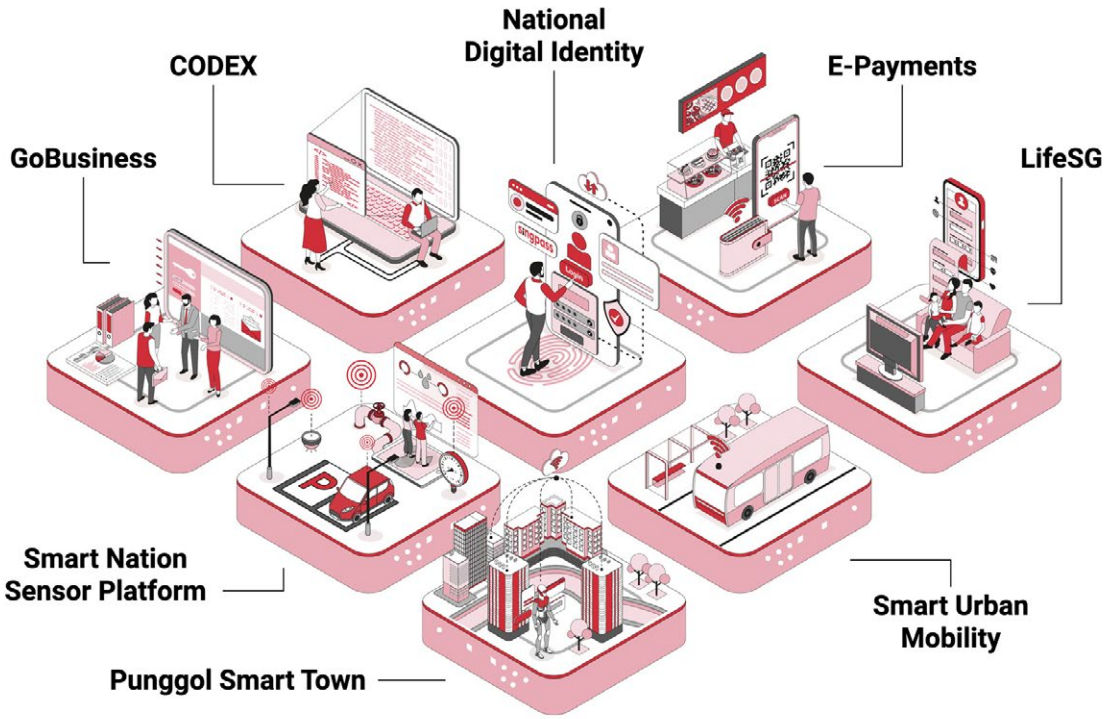
Урядовий хмарний проект Сінгапуру (GIP) був запущений у 2016 році. Метою проекту було створення централізованої платформи для урядових агенцій для розміщення їхніх додатків та даних. Обсяг проекту включає надання безпечної, надійної та масштабованої хмарної інфраструктури, яку можуть використовувати урядові агенції. Метою проекту є також зменшення витрат, підвищення ефективності та покращення якості державних послуг.

62 Cloud security guidance. https://www.ncsc.gov.uk/collection/cloud/the-cloud-security-principles

63 Data protection impact assessments. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/

Одним з ключових каталізаторів хмарних технологій Сінгапуру є «Платформа розумної нації» (Smart Nation Platform, SNP)[64], яка включає національну інфраструктуру зв'язку та датчиків стеження, забезпечує централізовану агрегацію та обмін даними.

У рамках проекту уряд Сінгапуру забезпечив інтегровану та централізовану інфраструктуру[65], яка дозволяє урядовим агенціям швидко розгортати та керувати додатками, а також забезпечує масштабування, високу доступність та безпеку даних. Це дозволяє урядовим агенціям зосередитись на наданні кращих державних послуг громадянам та підприємствам, а також забезпечити швидку та ефективну взаємодію між різними урядовими агенціями. Завдяки цьому проекту, уряд Сінгапуру зміг зменшити витрати на IT інфраструктуру та забезпечити підвищення ефективності та якості державних послуг для громадян та підприємств.



Ініційований Агентством з розвитку інформаційних технологій Сінгапуру (Infocomm Development Authority of Singapore, IDA) та запущений SPRING Singapore, стандарт SS 584 (MTCS) встановлює доволі жорсткі вимоги до безпеки та операційних характеристик постачальників хмарних послуг з метою сприяння прийняттю зваженого управління ризиками та практик безпеки.

Стандарт SS 584 (MTCS) вирішив такі задачі для Сінгапуру:

- став стандартом, яким можуть керуватися постачальники хмарних послуг для того, щоб забезпечити належний рівень безпеки, конфіденційності даних. Раніше саме з цього приводу виникали побоювання зі сторони користувачів, а також недовіра зі сторони бізнесу;
- забезпечив прозорість та надав можливість користувачам оцінювати ризики, які виникають при використанні хмарних послуг на кожному із рівнів.

Стандарт SS 584 (MTCS) інтегрований з міжнародними стандартами. З огляду на те, що в державних реєстрах здійснюється обробка саме персональних даних, особливої уваги заслуговує відповідність

64 Using Data to Build a Better Future. https://www.smartnation.gov.sg/initiatives/strategic-national-projects/smart-nation-sensor-platform

65 Strategic National Projects. https://www.smartnation.gov.sg/initiatives/strategic-national-projects

міжнародному стандарту щодо захисту персональних даних ISO/IEC 27001. Це формує гарантії того, що суб'єктам персональних даних, чиї дані оброблюються із використанням хмарних технологій, будуть забезпечені: належне видалення даних; суверенітет даних; мобільність даних; відповідальність за порушення, пов'язані із даними; доступ до даних; безперебійність бізнесу, який здійснює обробку даних; відновлення даних внаслідок інцидентів; управління інцидентами, пов'язаними із даними.

SS 584 (MTCS) охоплює 535 безпекових контролів для трьох різних рівнів безпеки у хмарі.

TIER / РІВЕНЬ 1:

Призначений для некритичних даних та систем, які мають базовий рівень безпеки, що враховує ризики та загрози безпеці, які спрямовані на системи з низьким рівнем впливу. (наприклад: хостинг веб-сайту з публічною інформацією).

TIER / РІВЕНЬ 2:

Призначений для організацій, які використовують хмарні сервіси для захисту бізнесової або особистої інформації та запускають критичні бізнес-дані та системи в інформаційних системах середнього рівня впливу. Постачальники хмарних послуг на цьому рівні мають більш жорсткі заходи безпеки (наприклад: Email / CRM - системи управління взаємовідносинами з клієнтами).

TIER / РІВЕНЬ 3:

Призначений для компаній зі специфічними потребами та більш жорсткими вимогами до безпеки. Для адресування ризиків та загроз безпеці в інформаційних системах з високим рівнем впливу, які використовують хмарні сервіси, можуть також застосовуватися галузеві регулятивні вимоги (наприклад, фінансові / медичні дані).

Стандарт SS 584 (MTCS) вирішує такі задачі:

- надає постачальникам хмарних послуг належний рівень безпеки, конфіденційності даних. Раніше саме з цього приводу виникали побоювання зі сторони користувачів, а також недовіра зі сторони бізнесу;
- забезпечує прозорість та надає можливості користувачам оцінювати ризики, які для них виникають при використанні хмарних послуг на кожному із рівнів.

Також Стандарт SS 584 (MTCS) надав можливість користувачам оцінювати можливості того чи іншого постачальника хмарних послуг з точки зору дотримання мінімальних безпекових стандартів.

Урядова хмарна інфраструктура Ізраїлю

Проект Ізраїльської урядової хмари (GovIL) був запущений в 2013 році з метою забезпечення безпечної, надійної та економічної хмарної інфраструктури для урядових агентств. Проект включав широкий спектр хмарних сервісів, таких як IaaS, PaaS та SaaS, і мав на меті поліпшити ефективність, зменшити витрати та збільшити гнучкість урядових агентств. Крім того, проект спрямовувався на покращення безпеки та конфіденційності урядових даних та додатків за допомогою впровадження строгих протоколів безпеки та найкращих практик.

Урядова хмарна стратегія, оприлюднена 11 грудня 2022 року, була сформульована в рамках проекту «Німбус» спільними зусиллями Національного цифрового агентства, Держзакупівель, Національного кіберагентства, Директора з бюджету Міністерства фінансів та Відділу уряду та суспільства в Офісі Прем'єр-міністра. Проект «Німбус» розділений на чотири частини з чотирма окремими тендерами: на будівництво дата-центрів та надання хмарних послуг уряду на публічній платформі – переможцями стали *Google та Amazon Web Services (AWS)*; на допомогу у складанні стратегії уряду з переходу до

хмарних технологій; на надання технічної допомоги при впровадженні переходу до хмарних технологій; та, який поки не оприлюднений, на надання послуг щодо оптимізації використання хмарних технологій.

У нещодавньому дослідженні[66], замовленому компанією Google, AlphaBeta (частина Access Partnership) оцінила приріст продуктивності економіки, який відбувається при створенні *«регіону Google Cloud»* в Ізраїлі. Основні повідомлення з дослідження: 1) очікується, що створення *регіону Google Cloud* в Ізраїлі сприятиме зростанню ВВП на суму 7,6 мільярдів доларів США між 2022 і 2030 роками, та дозволить створити 21 200 робочих місць до 2030 року; 2) збільшення інвестицій у хмарні технології в державному секторі між 2022 і 2030 роками очікується мати ефект, еквівалентний збільшенню витрат на громадське здоров›я на суму приблизно 1,3 мільярда доларів США щорічно.

Сполучені Штати: від Cloud First до Cloud Smart

У 2019 році федеральним урядом Сполучених Штатів була схвалена оновлена «розумна хмарна» стратегія. У звіті для Президента США про модернізацію федеральних IT-систем[67], оприлюдненому у 2017 році, Адміністративно-бюджетне управління (OMB) пообіцяло оновити застарілу урядову Федеральну стратегію хмарних обчислень («Cloud First»). Виконуючи цю обіцянку, Адміністрація розробила нову стратегію для прискорення прийняття агентствами хмарних рішень **«Cloud Smart»**.

Розроблена майже через десять років після свого попередника, стратегія «Cloud Smart надає агентствам корисну інформацію, рекомендації та широкі повноваження для впровадження хмарних рішень. Нова стратегія базується на трьох основних стовпах успішного впровадження хмари: **безпека, закупівлі та кваліфікований персонал**.

Стратегія Cloud Smart заохочує агентства **розглядати хмару як набір рішень, які пропонують багато можливостей і опцій управління для покращення виконання завдань та надання послуг**. Крім того, Cloud Smart працює за принципом, згідно з яким **агентства повинні мати можливість оцінити варіанти хмарних рішень на основі своїх потреб у послугах і завдань, технічних вимог і існуючих регуляторних обмежень**.

Федеральна програма управління ризиками та авторизацією (FedRAMP) забезпечує стандартизований підхід до оцінки безпеки, авторизації та постійного моніторингу хмарних сервісів, які використовуються федеральними урядовими установами США.

Документ[68] визначає елементи управління відповідно до **трьох рівнів впливу (наслідків від втрати конфіденційності, цілісності, доступності інформації): низького, середнього та високого**. На кожний рівень впливу NIST встановлює технічні вимоги[69]. NIST забезпечує підтримку та оновлення керівних принципів та технічних стандартів, що становлять основу системи оцінювання FedRAMP. Особлива увага приділяється документу «NIST SP 800-53»[70], який містить засоби контролю за безпекою та конфіденційністю для федеральних інформаційних систем і організацій. Чим вищий рівень впливу, тим більше базових засобів контролю потрібно: 123 елементи контролю для систем з низьким рівнем впливу, 325 – для систем з помірним впливом і 421 – для систем з високим впливом. Ризики з низьким рівнем впливу включають дані, які призначені для загального використання, тому будь-яка втрата даних не пошкодить місію, безпеку, фінанси або репутацію агентства. Ризики з помірним впливом

66 Google Cloud Region: Lifting Productivity in the Israeli Economy. https://accesspartnership.com/google-cloud-region-lifting-productivity-in-the-israeli-economy/

67 https://www.whitehouse.gov/wp-content/uploads/2018/03/E.O.-13800-Report-Final.pdf

68 Understanding Baselines and Impact Levels in FedRAMP. https://www.fedramp.gov/understanding-baselines-and-impact-levels/

69 Standards for Security Categorization of Federal Information and Information Systems. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

70 Security and Privacy Controls for Information Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

включають дані, які не доступні для громадськості, наприклад особисту інформацію, тому порушення може серйозно вплинути на діяльність агентства. **Більшість федеральних установ США працюють на середньому рівні впливу, оскільки вони використовують «контрольовану несекретну інформацію»**, у 2017 році майже 80% заявок FedRAMP були на цьому рівні.

Оцінки FedRAMP зосереджені на конкретних хмарних сервісах. **FedRAMP оцінює та авторизує не компанії в цілому, а їхню «пропозицію хмарних послуг» (CSO) на певних рівнях впливу.** Кожна організація проходить кілька оцінок перед затвердженням. Кожен звіт про оцінку готовності CSO (RAR) оцінюється в рамках «межі авторизації», яка є оглядом внутрішніх служб, компонентів та інших пристроїв, а також підключень до зовнішніх служб і систем. Якщо необхідно, RAR детально описує, які зміни надавач послуг повинен буде внести (і підтвердити), перш ніж її CSO буде вважатися прийнятною.

Сертифікація FedRAMP не закінчується після отримання сертифікату. Після того, як організація отримала сертифікат FedRAMP, вона повинна щорічно проходити повторну оцінку. Крім того, деталі щомісячного моніторингу мають бути надані до **Спільної авторизаційної ради (JAB), яка є органом, що приймає рішення в рамках FedRAMP**. Наприклад, надавачі хмарних послуг з середнім/високим рівнем впливу мають виправляти всі виявлені ризики з високим рівнем впливу протягом 30 днів, ризики з середнім - за 90 днів, а з низьким - за 180 днів.

FedRAMP використовує для оцінки сторонніх експертів (третю сторону), які самі відповідають вимогам FedRAMP та стандарту ISO/IEC 17020. Вони оцінюють здатність CSO підтримувати чітко визначені межі системи, описувати внутрішні та міжсистемні процеси, керувати потоками конфіденційних метаданих та даних користувачів, ризики, пов'язані з взаємозв'язками, які використовуються для передачі федеральних або конфіденційних даних, а також ризики, пов'язані з використанням зовнішніх систем та служб, які не авторизовані FedRAMP.

У 2020 році JAB FedRAMP включив локалізацію даних як необов'язкову вимогу для FedRAMP високого рівня впливу, щоб забезпечити сумісність вимог між FedRAMP та Посібником з вимог безпеки (SRG) Міністерства оборони США[71], який є внутрішнім документом Міністерства оборони для авторизації надавачів хмарних послуг. Рівень впливу DOD SRG 4 майже ідентичний з FedRAMP високого рівня впливу, за винятком вимоги щодо локалізації даних. JAB та Агентство інформаційних систем Міністерства оборони досягли компромісу, за яким JAB додав можливість локалізації даних до FedRAMP високого рівня впливу, а відповідно Міністерство оборони надало визнання (дозвіл) на рівні SRG 4 будь-якому CSO, що авторизовано на FedRAMP високого рівня впливу.

Незважаючи на те, що офіс управління програмою FedRAMP різко скоротив час, необхідний для авторизації постачальника хмарних послуг, ще потрібно вирішити основні проблеми, які сприяють відносно повільному темпу оцінювання. Наприклад, **відсутність взаємного визнання між агентствами під час прийняття дозволів FedRAMP призвела до значного дублювання зусиль під час оцінки безпеки для розгортання хмарної інфраструктури**. Крім того, через велику кількість специфічних процесів для агентств складно видавати дозвіл на експлуатацію для рішень, навіть якщо залучаються існуючі авторизовані надавачі хмарних послуг.

Cloud Smart пропонує двосторонній підхід до розумнішого придбання та використання хмарних сервісів федеральними відомствами за допомогою вдосконалення використання SLA (Угоди про рівень обслуговування) між замовником і постачальником послуг. Хоча це ще не стандартизовано в Федеральному положенні про закупівлі (FAR), положення угоди про рівень обслуговування включаються в розділи контракту щодо гарантії якості. **Очікувана стандартизація SLA має забезпечити більшу ефективність хмарних закупівель для агентств, дозволить детально сформулювати ролі та обов'язки, встановити чіткі показники ефективності та впровадити плани усунення невідповідності.**

71 DoD Cloud Computing Security. https://public.cyber.mil/dccs/

Рекомендації

Нижче подаються структуровані рекомендації, що стосуються:

1) розробки національної хмарної стратегії України;
2) проектних умов для урядової хмарної інфраструктури;
3) структури проектного менеджменту з розбудови урядової хмарної інфраструктури;
4) необхідних умов угоди про рівень обслуговування щодо захисту персональних даних;
5) вибору місця «приземлення» хмарних послуг і локалізації резервних копій державних інформаційних ресурсів за кордоном.

Рекомендації для розробки національної хмарної стратегії

У Практичному посібнику із безпечного розгортання урядових хмар[72] Європейської агенції з мережевої та інформаційної безпеки (ENISA, 2013), пропонуються рекомендації, які були і залишаються актуальними для розробки хмарної стратегії України:

- Необхідно розробити стратегію з керівними принципами високого рівня, яка охоплює технічні, юридичні та організаційні питання перед впровадженням хмарних послуг. Для цього потрібно чітко визначити модель управління хмарною ініціативою. План впровадження повинен бути послідовним та містити цілі та бачення урядових органів. Гнучке поширення хмарних послуг в декількох державних установах може бути реалізовано за умови визначення централізованої стратегії. Відсутність стратегії та дефіцит технічних, правових і процедурних аспектів є критичними перешкодами для запуску державних хмарних послуг.
- Необхідно розглянути програму, яка передбачатиме поступове впровадження безпечних хмарних послуг з покроковим планом виконання та значущими результатами та етапами. «Крок за кроком» план може бути варіантом для поступового впровадження хмарних послуг в державних секторах. Цей підхід полягає в довірі до технологій протягом м'якого переходу та дозволяє державним установам засвоїти новий спосіб управління та розгортання IT-сервісів і основних процесів для IT-операцій. Поступове впровадження забезпечить більш ефективне використання хмарних послуг та допоможе уникнути негативних наслідків, пов'язаних зі змінами в державному секторі.
- Розробити обґрунтовану та ризик-орієнтовану політику, яка буде сприяти запровадженню хмарних технологій у державних секторах та використанню загальнодоступних хмарних рішень для відкритих даних. Політика має допомогти урядовим органам вибирати оптимальні хмарні обчислення для своїх послуг. Політика *Cloud First* рекомендує урядовим організаціям спочатку розглянути та оцінити потенційні хмарні рішення перед тим, як робити будь-які нові інвестиції у нові послуги.

72 Good Practice Guide for securely deploying Governmental Clouds. https://www.enisa.europa.eu/publications/good-practice-guide-for-securely-deploying-governmental-clouds

- Пов'язати національну хмарну стратегію з проектами та ініціативами, які підвищують ефективність державних ІКТ та сприяють розвитку центрів обробки даних. Хмарні технології можуть сприяти зусиллям щодо консолідації центрів обробки даних та спрощення портфелю ІКТ, зменшуючи кількість додатків, які розміщені у державних центрах обробки даних.
- Оцінити можливість розгортання публічної хмари. Публічна хмара може бути більш життєздатним варіантом для державного сектора, якщо вдасться вирішити питання безпеки та інших проблем, і використовувати переваги, які пропонує парадигма хмарних обчислень. Публічні хмари можуть бути розгорнуті для некритичних послуг на другому етапі реалізації стратегії хмарних обчислень із покроковим плануванням виконання.
- Країни-члени повинні забезпечувати відповідність стратегії національним законам, нормативним актам та вимогам національного агентства щодо безпеки та захисту даних. Крім того, країни-члени повинні переконатися, що національна стратегія відповідає національним законам та нормам ЄС щодо безпеки та захисту інформації, активів та інфраструктури та враховує конфіденційність даних. Ми сприяємо прийняттю ЄС єдиного європейського набору правил та норм щодо безпеки та конфіденційності, щоб підтримати країни-члени у виконанні цих вимог.
- Оцінити можливості розробки державних каталогів послуг, які включатимуть гарантовані хмарні продукти/додатки та каталоги послуг, що поділяться за цільовими урядовими хмарними платформами, профілями використання та передовими методами.

Перехід на хмарні технології слід розглядати з точки зору проектного менеджменту як проект національного рівня, що потребує визначення проектних умов, планування завдань та злагодженого їхнього виконання.

З урахуванням дослідженого міжнародного досвіду та кращих практик впровадження урядової хмарної інфраструктури, можна запропонувати наступні проектні умови.

Рекомендації щодо проектних умов для урядової хмарної інфраструктури:

- Забезпечення безпечних, надійних та ефективних за вартістю хмарних сервісів для урядових агентств з метою впровадження цифрових послуг для громадян України, е-резидентів та установ.
- Забезпечення доступу до широкого спектру хмарних сервісів, включаючи SaaS, PaaS та IaaS, та «посольства даних» для покращення ефективності, зниження витрат та покращення якості, безпеки та стійкості урядових послуг.
- Створення гібридної та багатоплатформної інфраструктури для використання в секторі державного управління, повторного використання даних уряду, використання відкритих технологій та продуктів з програмним забезпеченням приватним сектором та створення майданчика для приватних постачальників IT-рішень та хмарних послуг.
- Покращення безпеки та стійкості, відповідності вимогам та управління ризиками для даних та застосунків.
- Встановлення пріоритету безпеки (безпека на етапі проектування), стійкості (стійкість на етапі проектування) та конфіденційності (конфіденційність на етапі проектування) за допомогою відповідних стандартів, протоколів та найкращих практик.

- Проект повинен забезпечити сталість дата-центрів відповідно до європейської зеленої угоди.
- Проект повинен забезпечити покращені рівні державної взаємодії, інтероперабельність інтегрованих високоякісних цифрових публічних послуг, яка дозволяє громадянам отримати до них доступ в рамках єдиного безперервного досвіду, заснованого на їх бажаннях та потребах.
- Проект буде оцінювати існуючі політики та розробляти та приймати нові правила та політики для України відповідно до *acquis* ЄС.

Рекомендації щодо структури проектного менеджменту з розбудови урядової хмарної інфраструктури

Ключовими елементами структури проектного менеджменту з розбудови урядової хмарної інфраструктури є такі:

- Визначення обсягу та цілей проекту: Першим кроком є визначення обсягу проекту. Це повинно включати визначення списку цифрових послуг та відповідних до них зацікавлених сторін в українському державному секторі, категорії даних, які використовуються для цих цифрових послуг, типи хмарних сервісів та очікувані результати проекту. Це допоможе визначити додаткові вимоги до хмарної інфраструктури.
- Встановлення рамок управління: Встановлення рамок управління є важливим для успіху проекту та його прозорості. Це повинно включати політики, стандарти та процедури управління хмарною інфраструктурою, відповідно до принципів відкритих даних уряду, обробки персональних даних та додатків. Рамки повинні також враховувати питання безпеки, відповідності вимогам та управління ризиками.
- Вибір правильної технології: Вибір правильної технології є ключовим для успіху проекту. Пріоритет повинен бути наданий використанню технологій та продуктів з відкритим вихідним кодом. Технологія повинна відповідати таким вимогам: (1) дозволяти найшвидше та ефективніше впровадження проекту, (2) бути сумісною з існуючими системами для обробки даних українського державного сектору. Хмарна інфраструктура також повинна бути масштабованою, гнучкою та стійкою.
- Вибір відповідної моделі розгортання: Модель розгортання повинна бути вибрана на основі конкретних потреб проекту. Існують чотири основні моделі розгортання: (1) публічний хмарний сервіс, (2) приватний хмарний сервіс, (3) колективний хмарний сервіс та (4) гібридний хмарний сервіс. Модель розгортання повинна враховувати питання безпеки, конфіденційності даних, вимог до регулювання, аналізу ризиків та оцінки впливу.
- Вибір постачальника хмарних сервісів: Процес повинен базуватися на прозорій процедурі закупівлі, яка проводиться відповідно до українського законодавства, що застосовується в цій сфері. Критерії вибору повинні включати: (1) корпоративну структуру такого постачальника та його систему відповідності, (2) технічні можливості, необхідні для створення хмарної інфраструктури та надання послуг відповідно до технологій та моделі розгортання, які будуть необхідні для впровадження проекту, (3) відповідність вимогам приватності, (4) оцінку безпеки, (5) можливості з технічного обслуговування та оцінки стану системи, (6) фінансові аспекти та бюджет, (7) інші аспекти, які можуть бути застосованими.
- Розробка плану міграції: Міграція до хмари може бути складним процесом. Ключовим є розробка плану міграції, який включає: (1) категоризацію даних та визначення найбільш оптимальної

технології, моделі розгортання, місця розташування та оптимальних заходів безпеки для подальшої обробки даних для надання цифрових послуг або для створення резервних копій, (2) кроки та терміни для переміщення даних та додатків до хмари, (3) видалення даних з попередніх пристроїв зберігання, якщо необхідно. План повинен також включати попереднє тестування та підтвердження, щоб забезпечити успішну міграцію.

- Забезпечення високого рівня прозорості, безпеки та стійкості: Ці аспекти є критичними для проектів урядової хмари, оскільки як уряди, так і великі корпорації, що надають хмарні послуги, стикаються з дефіцитом довіри. Інфраструктура повинна бути розроблена з кількома рівнями безпеки, включаючи фізичну, мережеву та захист даних, а також повинна бути прозорою. Вона також повинна бути високодоступною та стійкою, щоб мінімізувати час простою та забезпечити безперебійну роботу.

- Стосовно вартості та сталого розвитку: Витрати на проект повинні бути ретельно вивчені, а також потрібно розробити стійку модель фінансування. Проект також повинен враховувати довгострокові витрати на підтримку та оновлення інфраструктури. Потрібно розробити загальну стратегію хмарних технологій та план дій уряду для сприяння міграції до хмари з метою забезпечення технічної та операційної гнучкості та підвищення ефективності витрат.

- Стосовно розташування хмарної інфраструктури, вони повинні бути стратегічно розташовані, щоб забезпечити зв›язок та доступність. Вони також повинні бути розроблені таким чином, щоб мінімізувати ризик фізичних порушень під час тривалого збройного конфлікту, кібератак, перебоїв в роботі електромереж, природних катастроф та інших порушень. Для цих цілей необхідно оцінити політичні ризики, а також ризики захисту даних та критерії безпеки.

Рекомендації щодо необхідних умов угоди про рівень обслуговування стосовно захисту персональних даних

Договірна модель надання хмарних послуг передбачає укладення угоди SLA (Угоди про рівень обслуговування). SLA - це документ, який фіксує домовленості щодо рівня сервісу, який клієнт може очікувати від постачальника хмарних послуг. Угода встановлює умови, за якими постачальник хмарних послуг буде надавати свої послуги, включаючи рівень доступності, продуктивності, безпеки та конфіденційності. Угода також містить процедури взаємодії між постачальником та клієнтом у разі виникнення проблем, зокрема щодо усунення невідповідностей. SLA є важливим інструментом для забезпечення надійності та якості хмарних послуг. Клієнти можуть використовувати SLA для перевірки відповідності рівня послуг їх потребам та для забезпечення того, що постачальник хмарних послуг дотримується умов угоди.

Постановою Кабінету Міністрів України від 30 грудня 2022 р. № 1500[73] затверджено Порядок укладення SLA між власниками (держателями) державних інформаційних ресурсів (публічних електронних реєстрів) та надавачами хмарних послуг. Зокрема, встановлено, що договір укладається між замовником та надавачем послуг у письмовій формі та містить окрім типових договірних положень такі суттєві умови:

- Умови доступу замовника до даних, що обробляються під час виконання договору.

- Умови захисту даних з боку надавача послуг із розміщення даних на хмарних ресурсах та/або центрах обробки даних.

73 Постанова Кабінету Міністрів України «Деякі питання забезпечення функціонування державних інформаційних реурсів». https://www.kmu.gov.ua/npas/deiaki-pytannia-zabezpechennia-funktsionuvannia-derzhavnykh-informatsiinykh-t301222

- Вимоги щодо строку оповіщення сторін про інциденти кібербезпеки.
- Вимоги до забезпечення безперервності надання послуг із розміщення даних на хмарних ресурсах та/або центрах обробки даних.
- Умови передачі замовнику даних (інформації), зокрема їх резервних копій, що були накопичені, створені у процесі виконання договору.
- Умови видалення (знищення) даних (інформації), їх резервних копій, що були створені, накопичені та/або передані надавачу послуг у ході та для виконання договору.

Практика щодо договірного врегулювання правовідносин щодо надання приватними компаніями хмарних послуг для обробки даних із державних реєстрів продовжує формуватися, зокрема в ЄС. Протягом 2022 року, 22 органи захисту даних (DPAs) у країнах, що належать до Європейського економічного простору (ЄЕП), включаючи Європейського дата-захисника (EDPS), розпочали координовані дослідження[74] щодо використання хмарних сервісів публічним сектором. Усього були охоплені близько 100 державних установ у країнах ЄЕП, включаючи європейські інституції, що діють у різних сферах (наприклад, охорона здоров›я, фінанси, податки, освіта, покупці та постачальники IT-послуг).

Європейська рада із захисту даних (EDPB) схвалила звіт щодо результатів своєї першої спільної дії з контролю (Coordinated Enforcement Action,[75] 17.01.2023), присвячений використанню хмарних сервісів публічним сектором. EDPB підкреслює необхідність дотримання публічними органами повної відповідності GDPR та містить рекомендації для публічних секторів щодо використання хмарних продуктів або сервісів. Крім того, було опубліковано список заходів, які вже були прийняті контролюючими органами із захисту даних в галузі хмарних обчислень.

У звіті зазначається, що в більшості розслідуваних випадків CSP пропонували стандартні заздалегідь визначені контракти, і державним органам було важко домовитися про індивідуальний контракт. За таких обставин державні органи вимушені або прийняти умови, запропоновані в попередньо визначеному контракті, або не використовувати хмарний сервіс. Тому, щоб уникнути будь-яких потенційних порушень у сфері захисту персональних даних, важливо, щоб державні органи мали можливість узгодити умови контракту з CSP.

EDPB повідомляє, що коли різні державні органи ведуть переговори про однакові послуги від імені кількох державних органів, здається, що дисбаланс у переговорах зменшується, і, таким чином, є перевага використання колективної влади. EDPB також порадила, що офіцер із захисту даних (Data Protection Officer – DPO), який має бути і зі сторони державних органів як клієнтів, і зі сторони CSP, має відігравати активну роль в аналізі та переговорах щодо контрактів, які пропонують CSP.

У багатьох випадках централізована закупівельна організація (ЦЗО) обирає CSP. Таким чином, EDPB зазначає, що для ЦЗО важливо оцінювати послуги в першу чергу та пропонувати державним органам лише ті послуги, які відповідають стандартам із захисту персональних даних.

Зважаючи на процес євроінтеграції України, аналіз вищезгаданої практики в ЄС дозволяє сформулювати рекомендації для того, щоб розміщення персональних даних громадян України із державних реєстрів України на серверах за кордоном відповідало загальноєвропейським підходам. В перспективі це полегшить виконання Україною зобов'язань, які вона матиме перед ЄС на інтеграційному шляху та ставши членом ЄС.

74 Launch of coordinated enforcement on use of cloud by public sector. https://edpb.europa.eu/news/news/2022/launch-coordinated-enforcement-use-cloud-public-sector_en

75 Coordinated Enforcement Action, use of cloud-based services by the public sector. https://edpb.europa.eu/our-work-tools/our-documents/report/coordinated-enforcement-action-use-cloud-based-services-public_en

Нижче приведені ті аспекти, які вбачається важливим передбачити як необхідні умови для укладення контрактів з надавачами хмарних послуг:

1) **Визначити роль кожної із сторін у таких правовідносинах з огляду на специфіку сфери захисту персональних даних.**

Зазвичай, контрактні правовідносини передбачають визначення ролі кожної зі сторін на рівні «замовник» та «виконавець». Угоди, предмет яких передбачає обробку персональних даних, потребують окремого додаткового рівня регулювання – визначення ролі сторін щодо такої обробки. Саме це дозволить встановити права і обов'язки для кожної зі сторін, визначити зобов'язання перед суб'єктами даних, а також обрати належний транскордонний механізм передачі персональних даних.

Можливий такий розподіл ролей сторін:

Модель 1: контролер і оператор (процесор) персональних даних

Контролер – будь-яка фізична або юридична особа, суб'єкт владних повноважень чи будь-який інший орган, який самостійно чи спільно з іншими визначає цілі та засоби обробки персональних даних, а також інші фізичні або юридичні особи, для яких цілі та засоби обробки визначені законом.

Оператор (процесор) – будь-яка фізична або юридична особа, суб›єкт владних повноважень чи будь-який інший орган, який здійснює обробку персональних даних від імені контролера та уповноважена на це ним або законодавством.

Така модель є найрозповсюдженішою і найкоректнішою з точки зору управління персональними даними суб'єктів. Саме органи державної влади України, які відповідають за той чи інший реєстр, є контролерами персональних даних громадян України.

У державних органів є правовові підстави для збору та обробки персональних даних, а також на них покладені права та обов'язки:

- формувати мету збору та обробки даних,
- вжити відповідних і достатніх технічних та організаційних заходів, які забезпечують: належне та ефективне виконання принципів обробки персональних даних, дотримання підстав обробки персональних даних, інтеграцію захисних гарантій в процес обробки персональних даних,
- визначати категорії та обсяг персональних даних, які необхідні для досягнення мети, а також обсяг і строк обробки таких даних,
- встановлювати режим доступності даних, тобто визначати процесорів і суб-процесорів для обробки таких даних.

В свою чергу, в такій моделі надавачі хмарних послуг будуть процесорами (операторами) даних. Тобто, вони діятимуть цілком і повністю відповідно до інструкцій контролера. Тож це надасть можливість запобігти ситуаціям, коли надавачі хмарних послуг будуть використовувати дані для досягення власної мети, передаватиму дані третім особам без дозволу контролера тощо.

Важливо зазначити, що у громадян України як суб'єктів персональних даних буде можливість належним чином реалізувати свої права, пов'язані з обробкою персональних даних, зокрема право на доступ до персональних даних тощо. Для цього потрібно буде звернутися до контролера даних.

Для реалізації такої моделі необхідно додатково до SLA, в якому будуть визначені комерційні, організаційні та технічні умови співпраці, укласти угоду про передачу персональних даних. В такій угоді потрібно визначити ролі сторін як контролер і оператор (процесор), а також врегулювати взаємні права

та обов'язки щодо обробки персональних даних громадян України. Варто зазначити, що на основі такої угоди державні органи отримають можливість залучати додаткових операторів (процесорів) персональних даних (наприклад, якщо виникне потреба у збільшенні обсягу ресурсів І залученні інших надавачів хмарних послуг на підставі окремих SLA). Також за допомогою такої угоди можна залучати суб-процесорів персональних даних, якщо це буде необхідно (наприклад, якщо обробку персональних даних здійснюватиме по факту компанія, яка афілійована із надавачем хмарних послуг, або ж якщо умовами SLA буде передбачено залучення субпідрядників надавачами хмарних послуг).

Модель 2: спільні контролери

Спільні контролери – статус у правовідносинах між контролерами персональних даних, який визначається формуванням цілей та засобів обробки персональних даних двома або більше контролерами спільно.

Принциповою різницею із Моделлю 1 буде те, що в цій моделі державні органи і надавачі хмарних послуг будуть спільно визначати, яким чином відбуватиметься обробка персональних даних, а також розподілятимуть обов'язки щодо дотримання вимог обробки персональних даних. Це призводить до певної залежності державних органів від позиції надавачів хмарних послуг, тому така модель не рекомендується до застосування.

Для врегулювання правовідносин щодо обробки персональних даних також буде необхідно укласти окремий договір про розподіл обов'язків щодо дотримання вимог обробки персональних даних. Такий догорів має надаватися на запит громадян України, чиї дані підлягають обробці.

При цьому така модель щодо обробки персональних даних не вплине на реалізацію громадянами України своїх прав, пов'язаних з обробкою персональних даних. Державні органи та надавачі хмарних послуг повинні будуть в договорі визначити, хто з них як контролер є відповідальним за комунікацію з громадянами України. При цьому громадяни можуть звернутися до будь-якого з контролерів за реалізацією своїх прав.

Модель 3: незалежні контролери

Особливістю цієї моделі буде те, що і державні органи, і надавачі хмарних послуг будуть незалежно визначати цілі та засоби обробки персональних даних. Така модель не рекомендована до застосування у правовідносинах щодо використання хмарних послуг для обробки персональних даних із державних реєстрів, зважаючи на таке:

- у надавача хмарних послуг буде можливість використовувати персональні дані із іншою метою, аніж яка встановлена при зборі та обробці персональних даних державними органами. При цьому необхідно буде визначити окремі правові підстави для обробки даних надавачем хмарних послуг, а також належним чином проінформувати громадян як суб'єктів персональних даних про таку обробку їх даних,
- державні органи не матимуть повного контролю над діями надавача хмарних послуг із обробки таких даних, не зможуть вимагати видалення даних, забороняти передачу персональних даних третім особам тощо,
- за реалізацією своїх прав, пов'язаних зі збором та обробкою персональних даних, громадяни будуть вимушені звертатися не лише до державних органів, а і до надавачів хмарних послуг.

У випадку, якщо така модель правовідносин щодо персональних даних буде погоджена, потрібно буде визначити це в окремій угоді про передачу персональних даних, яка додаватиметься до SLA.

2) Провести DPIA (data processing impact assessment) – здійснити оцінку впливу обробки персональних даних (див. Додаток В).

Контролер зобов›язаний здійснити оцінку впливу обробки персональних даних на захист персональних даних до початку такої обробки, якщо використання нових технологій або характер, обсяг, контекст та цілі обробки ймовірно призведуть до настання ризику високого рівня для прав та свобод фізичної особи.

При визначенні того, чи потрібно здійснювати таку оцінку, потрібно звернути увагу на:

- категорії персональних даних, які підлягають обробці (якщо здійснюється обробка чутливих персональних даних, проведення оцінки є обов'язковим),
- випадки, за яких проведення такої оцінки є обов'язковим (це повинно бути визначено у законодавстві України),
- інші обставини, які варто взяти до уваги.

Зокрема такою обставиною є залучення надавача хмарних послуг до обробки персональних даних із державних реєстрів, в тому числі за кордоном. За загальним правилом відповідно до положень проекту закону України від 25.10.2022 N° 8153 «Про захист персональних даних» [76] не потрібно здійснювати оцінку впливу обробки персональних даних у випадках, якщо обробка персональних даних державними органами виникає внаслідок необхідності виконання завдань в суспільних інтересах або повноважень, покладених на контролера законом, а також якщо обробка персональних даних передбачена законом, процес прийняття якого включав оцінку впливу обробки на захист персональних даних.

Незважаючи на це, вважаємо за доцільне рекомедувати здійснення такої оцінки, так як відбуватиметься залучення надавача хмарних послуг до процесу обробки персональних даних, в тому числі за кордоном, що призводить до зміни ризиків відповідної обробки даних. Більше того, рекомендується проведення оцінки до того, як завершиться тендерний відбір надавача хмарних послуг, так як кожен із таких надавачів буде пропонувати певну сукупність організаційних та технічних заходів обробки персональних даних, що буде мати визначальний вплив на результати оцінки.

Більше того, рекомендується звернутися до контролюючих органів України у сфері персональних даних за відповідною консультацією щодо того, які заходи потрібно вжити.

Саме на основі результатів оцінки потрібно буде сформувати фінальні вимоги щодо організаційних і технічних заходів обробки персональних даних, які потрібно покласти в основу угоди про передачу персональних даних між державними органами і надавачами хмарних послуг.

Також потрібно здійнювати перегляд такої оцінки впливу. Відповідно до проекту закону України від 25.10.2022 N° 8153 «Про захист персональних даних» рекомендується проводити такі перегляди «з розумною періодичністю», але не рідше одного разу на три роки. Тож у цьому випадку можна здійснювати перегляд за зміни суттєвих умов співробітництва із надавачем хмарних послуг, а також визначити періодичність перегляду, зважаючі на інші особливості проекту.

3) Визначити, кому належать дані, в тому числі персональні, як актив.

Такий розподіл необхідно провести з метою встановлення взаємних прав і обов'язків щодо таких даних між державними органами та надавачами хмарних послуг. Це безпосердньо вплине на систему доступів до даних, порядок видалення даних тощо.

76 Проект Закону про захист персональних даних. https://itd.rada.gov.ua/billInfo/Bills/Card/40707

Особливо важливою є категорія персональних даних. Звертаємо увагу на те, що стосовно таких даних сторони повинні окремо врегулювати права і обов'язки, в залежності від ролей, які будуть між ними визначені. Детальніше про можливі моделі зазначено вище.

При цьому варто врегулювати це питання і по відношенню до даних, які не відносяться до категорії персональних. Наразі із розвитком технологій машинного навчання будь-які впорядковані сукупності даних можна потенційно використати із власною метою, яка буде відрізнятися від умов договору щодо надання хмарних послуг. Також потрібно пам'ятати про те, що персональні дані, обробка яких здійснювалась в хмарі, можуть бути анонімізовані. Це призведе до того, що такі дані не будуть вважатися персональними, та все ж їх структурованість і форма, в якій дані будуть представлені після анонімізації, може дозволити використання таких даних, наприклад, з метою розвитку та удосконалення технологій машинного навчання.

4) **Узгодити форму і порядок надання інструкцій надавачу хмарних послуг щодо обробки персональних даних. Пропрацювати можливі додаткові процеси із обробки персональних даних, які можуть бути ініційовані надавачем хмарних послуг незалежно в якості контролера даних. Передбачити порядок погодження залучення надавачем хмарних послуг субпроцесорів персональних даних, а також узгодити можливість заперечувати проти такого залучення.**

Це цілком залежатиме від моделі співробітництва сторін щодо обробки персональних даних, визначених вище. Такі умови потрібно детально передбачити в угоді щодо передачі персональних даних.

У випадку, якщо цього зроблено не було, є ризик виникнення конфліктів між сторонам у ході співпраці, а також ризики безпосередньо для суб'єктів персональних даних.

Більше того, у цьому випадку мається на увазі не лише те, що сторони повинні визначити вищевказані умови на договірному рівні, але і передбачити (і навіть протестувати) їх фактичне виконання. Це надасть можливість якісного і безперебійного надання хмарних послуг, а також мінімізує ризики, пов'язані із обробкою персональних даних.

Щодо форми і порядку надання інструкцій потрібно розробити шаблони таких інструкцій, задокументувати порядок надання і прийому інструкцій сторонами, визначити контактних осіб, адреси (електронні і фізичні) для належного оповіщення, домовитися про канали комунікацій, частоту комунікацій.

При визначенні можливих додаткових процесів із обробки персональних даних, які можуть бути ініційовані надавачем хмарних послуг незалежно в якості контролера даних, варто також оцінити всі можливі ризики для суб'єктів персональних даних. За наявності таких ризиків не рекомендується такий формат співробітництва, який би дозволяв надавачеві хмарних послуг такі можливості (модель «незалежні контролери» персональних даних). Відповідні ризики такої моделі зазначені вище.

Передбачити порядок погодження залучення надавачем хмарних послуг субпроцесорів персональних даних також вбачається важливим. Найбільш сприйнятливими є варіанти:

- надавачеві хмарних послуг заборонено залучення будь-яких субпідрядників (які щодо персональних даних можуть виступати субпроцесорами) до надання хмарних послуг,
- надавачеві хмарних послуг дозволено залучення в якості субпроцесорів персональних даних винятково афілійовані компанії із рівнем захисту персональних даних не нижчим, ніж у надавача хмарних послуг.

5) Обумовити категорії, обсяг, характер та мету обробки персональних даних, а також порядок їх видалення.

Реалізуючи проект щодо використання хмарних послуг для обробки персональних даних, розміщених в державних реєстрах, сторонам важливо не лише врегулювати взаємні права і обов'язки, а й вид та категорії персональних даних, які підлягають обробці, строк, характер та мету обробки, вид та категорії суб'єктів персональних даних, чиї дані підлягають обробці, та права і обов'язки контролера. Як зазначалося вище, найбільш сприятливою є Модель 1, за якої державний орган є контролером персональних даних, а надавач хмарних послуг є оператором (процесором). Детальніше проаналізуємо, так як ці аспекти є взаємопов'язані.

Щоб зрозуміти, чи перевірити, що обробка персональних даних не є надмірною, пропонуємо керуватися таким алгоритмом:

a) Мета обробки персональних даних. Контролер повинен встановити мету обробки персональних даних. Обмеження мети є одним із ключових принципів обробки персональних даних. Персональні дані повинні збиратися для точно визначених, явних і легітимних цілей та не оброблятись у спосіб, що є несумісним з цими цілями. Контролер, зокрема, зобов'язаний визначити мету обробки персональних даних до початку їх збору та не може змінювати її після збору персональних даних без згоди суб›єкта персональних даних, крім випадків, коли нова мета є сумісною із первинною.

Для SLA і угоди про передачу персональних даних чітке визначення такої мети обробки персональних даних є надзвичайно важливим, так як в подальшому дозолить контролювати, щоб обробка не здійснювалась із іншою метою, а також щоб надавач хмарних послуг не встановлював іншої мети обробки даних самостійно.

b) Категорії персональних даних. Контролер повинен визначити, які категорії та обсяг персональних даних необхідні для досягнення визначеної мети. Кожен контролер зобов'язаний вжити відповідних і достатніх технічних та організаційних заходів для забезпечення того, що обробляються тільки ті персональні дані, які необхідні для точно визначеної легітимної мети обробки.

Концепція «чутливі персональні дані»

Загальноприйнятим є виокремлення із сукупності різних категорій персональних даних «чутливих» персональних даних. Це важливо, так як загалом обробка таких персональних даних є забороненою і дозволяється лише в окремих випадках, визначених законом про захист персональних даних.

Відповідно до проекту закону України від 25.10.2022 N° 8153 «Про захист персональних даних» до цієї категорії віднесені дані про расове або етнічне походження, політичні, релігійні або світоглядні переконання, членство в професійних спілках, а також генетичних та біометричних даних, даних, що стосуються здоров›я, статевого життя або сексуальної орієнтації. Також окремою є категорія персональних даних, пов›язаних з притягненням до кримінальної відповідальності, правопорушень, кримінальних проваджень та судимості, а також пов›язаних із цим заходів безпеки.

Приймаючи рішення про обробку таких даних, зокрема, щодо використання для цього хмарних послуг (в тому числі із транскордонною передачею таких даних) потрібно:

- визначити, чи наявні спеціальні умови, за яких обробка таких даних дозволяється,
- провести оцінку впливу обробки персональних даних,
- визначити відповідні ризики та скласти план їх мінімізації,

- в залежості від плану мінімізації ризиків – передбачити та вжити відповідні організаційні й технічні заходи, або відмовитися від транскордонної передачі таких даних, або відмовитися від обробки таких даних взагалі.

Конфіденційна інформація

Варто звернути увагу і на те, що дані, в тому числі і персональні дані, можуть бути віднесені до категорії «конфіденційної інформації», так як це є ширшим поняттям і визначає режим доступу до даних, а не їх правову природу. Щодо їх обробки потрібно дотримуватися спеціальних правил:

- Закон України від 02.10.1992 N° 2657-XII «Про інформацію»[77] визначає, що «конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом»,
- при цьому проект закону України від 25.10.2022 N° 8153 «Про захист персональних даних» врегульовує, які заходи щодо обробки персональних даних потрібно вживати, якщо щодо таких даних застосовується режим конфіденційності: (а) цілісність і конфіденційність даних визначені серед ключових принципів обробки персональних даних. Дані повинні оброблятися із вжиттям належних технічних та організаційних заходів в такий спосіб, що гарантує їх належну безпеку, включаючи захист від несанкціонованої або неправомірної обробки, випадкової втрати, знищення або пошкодження, (б) серед заходів для забезпечення безпеки персональних даних визначені безперервне забезпечення конфіденційності, цілісності, доступності персональних даних і стійкості систем і сервісів обробки.

Отже, якщо до даних, в тому числі персональних даних, застосовується режим «конфіденційності», державним органам, які відповідають за державний реєстр із такими даними, під час врегулювання умов використання хмарних послуг для обробки даних (в тому числі і з транскордонною передачею даних), потрібно подбати про:

- безпечне місце «приземлення» хмарних послуг, де для таких даних були б забезпечені конфіденційність і цілісність таких даних,
- включення до SLA та угоди про передачу даних положень щодо конфіденційності, режими доступів та інших організаційних й технічних заходів, які надавач хмарних послуг вживатиме по відношенню до персональних даних,
- чітку процедуру видалення даних після закінчення надання послуг із обробки даних надавачем хмарних послуг.

Інформація, яка становить державну таємницю

Як і у випадку із режимом «конфіденційності» по відношенню до даних (в тому числі персональних) може бути встановлено режим «інформації, яка становить державну таємницю». Регулювання цього режиму здійснюється відповідно до Закону України від 21.01.1994 N° 3855-XII «Про державну таємницю»[78]. Конкретні дані можуть бути віднесені до державної таємниці за ступенями секретності «особливої важливості», «цілком таємно» та «таємно», а також категорії інформації, щодо яких може бути встановлений такий режим.

77 Закон України «Про інформацію». https://zakon.rada.gov.ua/laws/show/2657-12#Tex

78 Закон України «Про державну таємницю». https://zakon.rada.gov.ua/laws/show/3855-12#Text

Слід зважати, чи віднесені дані в державному реєстрі, які планується обробляти з використанням хмарних послуг за кордоном, так як відповідно до законодавства України заборонена передача (переміщення) державних інформаційних ресурсів (публічних електронних реєстрів), які містять службову інформацію та інформацію, що становить державну таємницю, та їх резервних копій для розміщення на хмарних ресурсах та/або центрах обробки даних, що розташовані за межами України.

c) **Обсяг персональних даних.** Контролер повинен знати обсяг персональних даних, які підлягають обробці. Цей показник потрібен для того, щоб дотримуватися принципу мінімізації даних, так як склад та зміст персональних даних, що обробляються, повинен бути достатнім, адекватним, відповідним і ненадмірним відповідно до визначеної мети їх обробки.

Обсяг обробки персональних даних необхідно визначати і з огляду на те, щоб надалі реалістично здійснювати оцінку впливу обробки персональних даних, розраховувати відповідні ризики та планувати заходи щодо їх мінімізації, а також оперативно реагувати у випадку порушень щодо персональних даних.

З організаційної та технічної точки зору розуміння обсягу персональних даних надає можливість правильно врегулювати контрактні правовідносини із надавачем хмарних послуг щодо залучених ресурсів.

d) **Характер обробки.** Контролер повинен оцінювати характер обробки персональних даних. Такий критерій потрібно враховувати для того, щоб визначити належні технічні та організаційні заходи для забезпечення обробки персональних даних, а також гарантувати безпеку обробки персональних даних такого рівня, який є співмірний ризику обробки персональних даних для прав і свобод суб›єктів персональних даних із дотриманням принципу пропорційності.

Найвагомішими складовими цього критерію є види обробки персональних даних і частота такої обробки.

Види обробки персональних даних, визначені у проекті закону України від 25.10.2022 № 8153 «Про захист персональних даних» включають будь-яку дію або сукупність дій з персональними даними з використанням або без використання автоматизованих засобів, зокрема збирання, фіксація, упорядкування, структурування, зберігання, адаптація, зміна, відновлення, ознайомлення, псевдонімізація, профілювання, знеособлення, використання, розкриття шляхом передачі або поширення, або надання доступу у інший спосіб, групування або комбінування, обмеження, видалення або знищення.

Щодо частоти обробки можливі так варіанти: одноразова, на постійній основі або обробка, яка здійснюється із певною періодичністю. Це важливий показник для оцінки впливу обробки персональних даних, визначення ризиків, а також планування співмірних організаційних і технічних заходів при обробці персональних даних.

Для реалізації обробки персональних даних із державних реєстрів із використанням хмарних послуг за кордоном потрібно надати надавачу хмарних послуг як оператору (процесору) персональних даних здійнювати обробку даних шляхом їх зберігання, передачі (в тому числі, за кордон) і видалення виняткова на основі інструкцій, отриманих від державних органів України, які виступають контролерами таких даних.

Для державних органів як контролера даних необхідно визначити механізм передачі персональних даних за кордон. Обраний механізм залежатиме від місця «приземлення» хмарних послуг. Перевага повинна надаватися країнам, у яких забезпечено адекватний (належний) рівень захисту персональних даних. За умови, якщо персональні дані будуть передаватися в інші країни (навіть

якшо це здійснюватиме вже надавач хмарних послуг при передачі персональних даних своїм афілійованим компаніям) потрібно попередньо провести оцінку впливу транскордонної передачі персональних даних (transfer impact assessment). На основі такої оцінки державні органи повинні прийняти рішення про:

- транскордонну передачу даних із вжиттям відповідних організаційних й технічних заходів,
- узгодження із надавачем хмарних послуг обробки персональних даних на території іншої країни,
- відмову від транскордонної передачі таких даних взагалі.

Токож рекомендуємо визначити, чи будуть дані, які обробляються за кордоном надавачами хмарних послуг, копією (бекапом) даних, які міситься в державних реєстрах. Таке рішення повинно бути прийнято, зважаючи на всі політичні, організаційні й технологічні ризики обробки даних із прив'язкою до країни «приземлення» хмарних послуг. На цьому базуватиметься і вибір правильної технології, і вибір моделі розгортання хмари.

e) **Видалення персональних даних.** Контролер повинен визначити строки обробки персональних даних і передбачити їх видалення. Одним из ключових принципів обробки персональних даних є обмеження їх зберігання. Дані повинні зберігатись у формі, що дозволяє ідентифікацію суб'єкта персональних даних не довше, ніж це необхідно для цілей, в яких вони обробляються. Персональні дані можуть зберігатись більший період часу для цілей архівування в суспільних інтересах, цілей наукового чи історичного дослідження або статистичних цілей за умови вжиття технічних та організаційних заходів, які вимагаються для забезпечення дотримання прав і свобод суб›єкта персональних даних.

Зважаючи на це, державні органи як контролери даних повинні визначити, протягом якого строку потрібно здійснювати обробку персональних даних в державних реєстрах для того, щоб досягти відповідної мети, після чого персональні дані підлягають повному видаленню чи анонімізації. Цей строк повинен бути чітко передбачений і в угоді щодо передачі даних, яка буде укладена додатково до SLA. Також із надавачем хмарним послуг в SLA і угоді про передачу даних потрібно передбачити випадки, коли обробка персональних даних надавачем припиняється (наприклад, припинення договірних відносин, видалення персональних даних на стороні контролера, порушення у сфері персональних даних), а дані підлягають повному видаленню або анонімізації.

Також важливо заздалегідь визначити процедуру видалення таких даних або їх анонімізації, а саме передбачити на договірному рівні, які організаційні та технічні заходи сторони для цього вживатимуть, і строки такого видалення. Результати видалення або анонімізації даних потрібно відобразити у відповідних документах.

Якщо сторони не домовилися про процедуру видалення або анонімізації даних, це може призвести до ризиків блокування персональних даних у хмарі, подальшої незаконної обробки персональних даних, а також загалом втрати державними органами контролю над обробкою таких персональних даних.

Потрібно звернути увагу також на те, що після закінчення строків обробки або настанні інших підстав, за яких відбувається припинення обробки персональних даних, такі дані можуть або повністю видалятися або анонімізуватися надавачем хмарним послуг. Анонімізація як опція можлива лише у деяких випадках, рішення щодо цього контролеру доцільно приймати після здійснення аналізу наслідків таких дій, а також передбачити це в SLA та угоді про передачу даних.

6. Узгодити процедуру реалізації прав суб›єктів персональних даних.

Якщо для співробітництва буде обрано модель, за якої державні органи виступатимуть в якості контролера персональних даних, а надавачі хмарних послуг будуть операторами (процесорами) персональних даних, тоді саме на державні органи буде покладено зобов'язання щодо реалізації прав суб›єктів персональних даних, чиї дані знаходяться в державних реєстрах.

Одними із ключових принципів обробки персональних даних є законність, добросовісність та прозорість. Персональні дані повинні оброблятись на підставах, передбачених цим Законом. Персональні дані повинні оброблятися у спосіб, що передбачає належну поінформованість суб'єкта персональних даних про обробку його персональних даних (збір, використання та іншу обробку, її спосіб та обсяг), крім випадків, передбачених цим Законом, з метою забезпечення усунення непередбачуваного для суб'єкта персональних даних негативного впливу на нього від обробки персональних даних.

Тому державним органам буде необхідно:

- проінформувати суб'єктів персональних даних щодо залучення надавача хмарних послуг до обробки їх даних, надати всі деталі щодо цього,
- забезпечити право суб›єктів персональних даних на доступ до своїх персональних даних, право на видалення персональних даних, а також реалізацію їх інших прав (з організаційної і технічної точки зору),
- передбачити взаємодію із надавачем хмарних послуг для реалізації таких прав суб'єктів. Відповідні положення потрібно включити в SLA та угоду про передачу даних.

7) Передбачити зобов›язання призначити відповідальну особу з питань захисту персональних даних (data protection officer – DPO) для кожної із сторін.

У проекті закону України від 25.10.2022 N° 8153 «Про захист персональних даних» передбачено, що у випадку обробки персональних даних суб'єктом владних повноважень (в цьому випадку – Центральною виборчою комісією) контролер та оператор зобов›язані призначити відповідальну особу з питань захисту персональних даних.

Основним завданням таких осіб є забезпечувати дотримання законодавства в сфері персональних даних на рівні державного органу та надавача хмарних послуг відповідно, комунікувати та співпрацювати із контролюючими органами у сфері обробки персональних даних, а також контактувати із суб'єктами персональних даних.

Ключовою вимогою до діяльності таких осіб є їхня незалежність. Особи можуть виконувати інші обов'язки, але це не може призводити до конфлікту інтересів. Більше того, такі особи можуть бути найняті на контрактній основі для обслуговування потреб в сфері захисту персональних даних для контролера і оператора (процесора),

Визначено перелік обов'язків такої особи:

- надавати інформацію та рекомендації контролеру або оператору та працівникам, які безпосередньо залучені до обробки персональних даних, про їх обов'язки;
- здійснювати моніторинг дотримання вимог цього Закону, включаючи розподіл обов›язків, підвищувати рівень обізнаності працівників контролера або оператора з питань захисту персональних даних, які безпосередньо залучені до обробки персональних даних;
- надавати рекомендації щодо оцінки впливу на захист персональних даних та здійснювати моніторинг її виконання;

- співпрацювати з контролюючим органом;
- бути контактною особою для контролюючого органу з питань, пов'язаних з обробкою персональних даних, включаючи попередні консультації та інші питання;
- належним чином враховувати ризики, пов›язані із обробкою персональних даних, зважаючи на специфіку, обсяг, контекст і цілі обробки персональних даних.

Планується, що в рамках потенційної реалізації проекту із обробки даних державних реєстрів надавачами хмарних послуг за кордоном саме на рівні співпраці відповідальних осіб з питань захисту персональних даних відбуватиметься основний прогрес у проекті.

8. Умови залучення інших зацікавлених державних органів до співпраці.

19.04.2023 Уряд ухвалив постанову щодо використання Платформи для швидкого створення і керування державними реєстрами. Завдяки такому інструменту міністерства і державні органи України зможуть швидко й зручно створювати публічні реєстри і керуватимуть ними. Командам Міністерства цифрової трансформації та Держспецзв'язку доручено працювати над цим інноваційним рішенням. При цьому за інформацією[79] Уряду наразі в Україні є понад 450 державних реєстрів. 80% з них технологічно застарілі і вразливі до кібератак. Тож для того, щоб вирішити цю проблему, а також забезпечити реалізацію проекту, найбільш раціональним вбачається саме використання хмарних технологій, а також інтеграція різних державних реєстрів для забезпечення належного рівня безпеки даних, гарантування актуальності даних в реєстрах, скорочення витрат на фінансове забезпечення і обслуговування реєстрів й серерів, на яких відбувається обробка персональних даних з реєстрів.

9. Передбачити процедуру проведення регулярних аудитів.

В SLA рекомендується передбачити регулярні аудити надавача хмарних послуг – в залежності від характеру обробки персональних даних та ризиків, які будуть визначені на рівні проведення DPIA.

Також рекомендується передбачити можливість проведення аудитів, у тому числі із залученням зовнішніх аудиторів, у випадку порушень, пов'язаних із персональними даними, порушень відповідного законодавства у сфері персональних даних, а також об'єктивних підозр, що надавач хмарних послуг вчиняє такі порушення.

10. Перевірити надавача хмарних послуг на дотримання положень GDPR на стадії подачі надавачем заявки на проходження конкурсу на надання відповідних послуг на стадії держзакупівель.

Така перевірка може відбуватися шляхом включення відповідних критеріїв для подачі на тендер на надання послуг.

Надалі надавачі хмарних послуг можуть засвідчувати це шляхом надання відповідей на питання опитника, сертифікаціями в сфері захисту даних та кібербезпеки.

Більше того, можна передбачити можливість попереднього аудиту надавача хмарних послуг на предмет дотримання законодавства в сфері захисту персональних даних.

Окремо потрібно включити відповідні гарантії в SLA та угоду про передачу даних.

79 Мінцифри: Платформа для розгортання реєстрів стане основою для цифрової трансформації. https://shorturl.at/txBNX

11. Передбачити моделі передачі персональних даних, перевірити наявність механізмів для транскордонної передачі даних. Державний орган, який діє як контролер, повинен ретельно оцінити передачу, яку може здійснювати CSP (наприклад, шляхом визначення категорій переданих персональних даних, цілей, суб'єктів, яким дані можуть бути передані, і перелік третіх країн).

Рекомендуємо перед стартом проекту провести такий комплексний аналіз. Ключові елементи в якості прикладу приводимо нижче.

Транскордонна передача персональних даних із Державного рєстру виборців надавачу хмарних послуг

Проаналізуємо задачу, в рамках якої потрібно забезпечити обробку даних із Державного рєстру виборців надавачем хмарних послуг за кордоном. В такому випадку рекомендованою є модель, за якої Центральна виборча комісія, яка є розпорядником Державного реєстру виборців, виступатиме в ролі контролера даних, а надавач хмарних послуг – оператором (процесором) даних. Між сторонами буде укладена SLA та угода про передачу даних.

а) Щодо категорій даних, які передбачаються до обробки

В Законі України від 22.02.2007 № 698-V «Про Державний реєстр виборців»[80] вказано, що до Реєстру заносяться та в базі даних Реєстру зберігаються встановлені цим Законом відомості про виборця (персональні дані) таких видів:

- ідентифікаційні персональні дані виборця;
- персональні дані, які визначають місце та умови голосування виборця;
- службові персональні дані.

До ідентифікаційних персональних даних виборця, які однозначно визначають його особу, належать: прізвище; власне ім›я; по батькові; дата народження; місце народження; унікальний номер запису в Єдиному державному демографічному реєстрі.

До персональних даних, які визначають місце та умови голосування виборця, належать: виборча адреса виборця (при цьому виборчою адресою виборця, який відбуває покарання у вигляді арешту, позбавлення або обмеження волі, є адреса установи виконання покарань), номер виборчої дільниці, до якої віднесений виборець, відомості про постійну нездатність виборця пересуватися самостійно.

До службових персональних даних Реєстру належать: дата набуття виборцем громадянства України; дата припинення громадянства України; дата визнання особи недієздатною; дата поновлення дієздатності особи; дата смерті виборця або дата оголошення його померлим; дата скасування рішення суду про оголошення особи, включеної до Реєстру, померлою; службова відмітка про вибуття виборця із зареєстрованого місця проживання.

В угоду про передачу даних, яка укладатиметься додатково до SLA, потрібно включити всі категорії даних, які планується передавати, а також зазначити, які організаційні й технічні заходи потрібно вжити надавачеві хмарних послуг для кожної з таких категорій. Особливу увагу потрібно звернути на таке:

- категорії даних «виборча адреса виборця, який відбуває покарання у вигляді арешту, позбавлення або обмеження волі» та «відомості про постійну нездатність виборця пересуватися самостійно» є «чутливими персональними даними». Наразі ми не бачимо підстав забороняти транскордонну передачу таких даних,

80 Закон України «Про державний реєстр виборців». https://zakon.rada.gov.ua/laws/show/698-16

- персональні дані в Реєстрів виборців можуть вважатися конфіденційною інформацією, тож сторони повинні вжити відповідні заходи для належної обробки таких даних,
- наразі в Реєстрі виборців немає даних, які можуть підпадати під режим державної таємниці.

b) Щодо співмірності категорій даних до обробки і мети обробки таких даних

В Законі України від 22.02.2007 № 698-V «Про Державний реєстр виборців» вказано, що Державний реєстр виборців – автоматизована інформаційно-комунікаційна система, призначена для зберігання, обробки даних, які містять передбачені цим Законом відомості, та користування ними, створена для забезпечення державного обліку громадян України, які мають право голосу відповідно до статті 70 Конституції України (виборці). Тож метою обробки персональних даних в цьому випадку є саме «забезпечення державного обліку громадян України, які мають право голосу відповідно до статті 70 Конституції України». Саме набір персональних даних, який складається із вищевказаних категорій, уможливлює досягення такої мети, так як забезпечує повну ідентифікацію фізичної особи. Це важливо з точки зору реалізації принципу «однократності включення виборця до реєстру», так як виборче право – це особисті права людини.

В угоді про передачу даних між контролером та оператором (процесором) даних потрібно визначити вищевказану мету обробки даних, а також включити положення про недопущення обробки таких даних із іншою метою.

c) Щодо обсягу персональних даних

Обсяг персональних даних визначається в цьому випадку в сукупності із метою обробки даних, що містяться у Реєстрі. Так як метою є «забезпечення державного обліку громадян України, які мають право голосу». Надалі потрібно визначити, в якому обсязі передавати дані надавачу хмарних послуг. Це залежатиме від рішення контролера, яке він прийме на основі оцінки впливу обробки персональних даних.

Найбільш доцільним є варіант резервного копіювання даних для їх обробки надавачами хмарних послуг за кордоном. Центральна виборача комісія повинна мати можливість відновлення після можливого збою своїх серверів впродовж прийнятного часу. Резервне копіювання є важливою частиною операцій із захисту інформації та кібербезпеки. Розміщення резервних копій бази даних Реєстру виборців, її частин, персональних даних за межами адміністративної території України в захищеній інфраструктурі є одним із способів фізичної сегрегації для гарантування безпеки виборчої архітектури. Цим рішенням варто скористатися не лише з огляду на поточні ризики знищення, порушення цілісності, конфіденційності чи втрати доступу до державних інформаційних ресурсів в ході триваючого збройного конфлікту, а визнати це системним рішенням з побудови більш стійкої інформаційної інфраструктури.

d) Щодо характеру обробки

Для реалізації обробки персональних даних із Реєстру виборців із використанням хмарних послуг за кордоном потрібно надати надавачу хмарних послуг як оператору (процесору) персональних даних здійснювати обробку даних шляхом їх зберігання, передачі (в тому числі, за кордон) і видалення винятково на основі інструкцій, отриманих від Центральної виборчої комісії як контролера даних.

Як вказано вище, найбільш доцільним є варіант резервного копіювання даних із Державного реєстру виборців для їх обробки надавачами хмарних послуг за кордоном.

е) Видалення персональних даних

Рекомендуємо передбачити видалення персональних даних надавачем хмарних послуг відповідно до вказівки Центральної виборчої комісії як контролера даних, а також у випадку припинення правовідносин між сторонами.

Перевага повинна надаватися повному видаленню даних, результати якого повинні бути перевірені й задокументовані.

У SLA та угоді про передачу даних потрібно передбачити усі організаційні та технічні заходи із видалення персональних даних на стороні надавача хмарних послуг.

Рекомендації щодо вибору місця «приземлення» хмарної інфраструктури

У разі прийняття рішення щодо використання хмарних технологій для зберігання резервних копій даних із державних реєстрів за кордоном, що потребує відповідних змін у законодавстві України, необхідно буде провести відбір місця фізичного зберігання даних. Пропонуємо розглянути такі опції, проте можуть бути й інші рішення, які можна застосовувати як окремо, так і одночасно:

Модель 1 – «Цифрова амбасада». За цією моделлю дані із державних реєстрів можуть бути фізично розміщені в ЦОД за кордоном, але в той же час обчислювальні потужності дата центрів будуть розташовані на території дипломатичних установ України або в інших локаціях, прирівняних до такого статусу на підставі міждержавного договору за прикладом Естонії і Люксембургу (див. нижче). Таким чином, це буде прирівнюватися до розташування даних на території України відповідно до статусу дипломатичних установ України за кордоном.

«Цифрова амбасада» Естонії в Люксембурзі

Естонія обрала Люксембург місцем для зберігання даних державних ресєтрів за кордоном. Це рішення було прийнято в 2017 році в рамках зусиль Естонії щодо посилення кібербезпеки та захисту цифрової інфраструктури. Угода між двома країнами дозволяє зберігати резервні копії даних Естонії в Люксембурзі, який вважається надійним і безпечним місцем для зберігання даних.

Це гарантує, що критично важливі дані Естонії залишаються в безпеці та доступні у разі кібератаки чи іншого інциденту безпеки.

За Угодою (див. Додаток):

1) приміщення центру даних є недоторканними і не підлягають обшуку, реквізиції, арешту чи виконавчим діям;

2) жодна посадова особа чи особа, яка виконує будь-які державні повноваження, не має права входити в приміщення без попереднього дозволу уповноваженого представника Естонської Республіки, крім випадків пожежі чи інших надзвичайних ситуацій, які потребують негайних захисних заходів і можуть становити загрозу для безпеки;

3) для захисту приміщень від будь-якого вторгнення або пошкодження на території Люксембургу необхідні заходи, які потребують попереднього дозволу уповноваженого представника Естонської Республіки;

4) обладнання та ліцензії, необхідні для роботи центру обробки даних, вважаються активами Естонської Республіки та користуються імунітетом від будь-якої форми судового процесу;

5) усі дані та інформаційні системи, що зберігаються Естонською Республікою в приміщеннях, вважаються державними архівами і користуються таким самим режимом, який надається дипломатичним представництвам щодо їх офіційних повідомлень та передачі документів;

6) для відправлення та отримання офіційних повідомлень Естонська Республіка може використовувати дипломатичних кур›єрів, яких вона уповноважила, а також код і шифрування у своїх офіційних повідомленнях.

Модель 2 – передача даних в ЦОД за кордоном з використанням програми обмеження витоку даних.

При використанні цієї моделі є такі фактори, що визначають вибір місця розташування ЦОД для зберігання та обробки даних:

- Політична складова.
- Технологічна складова.
- Режим захисту персональних даних. Механізми для транскордонної передачі персональних даних.
- Безпекові питання.

За цією моделлю, передбачається потреба у технологічному забезпеченні зберігання та обробки даних за визначеними фізичними локаціями. Таку можливість надає «Європейська програма обмеження витоку даних».

Програма обмеження витоку даних за межі ЄС

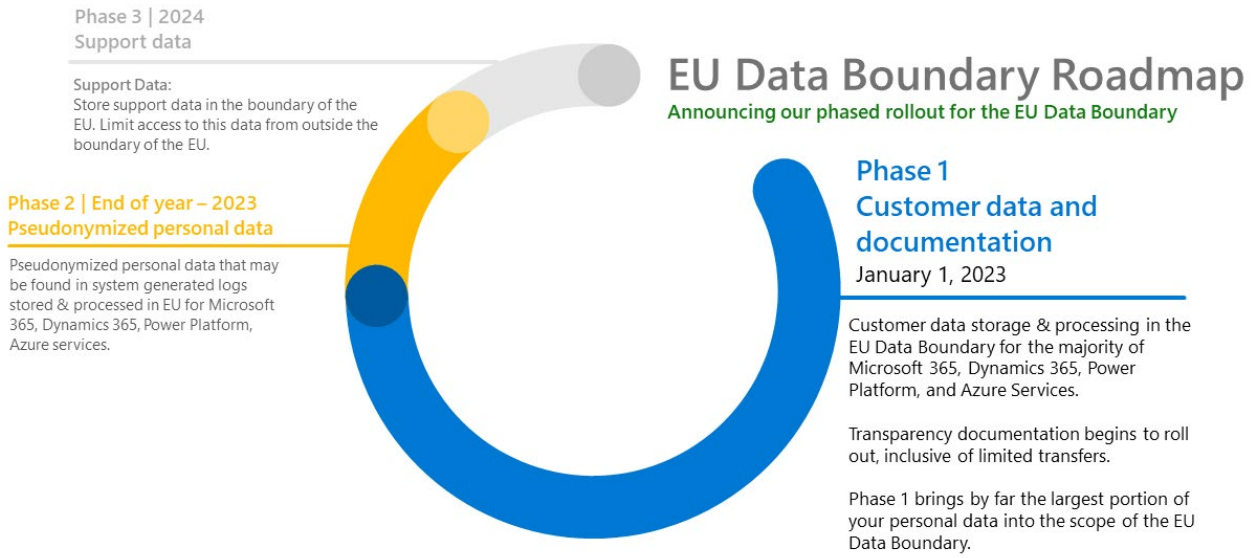
З 1 січня 2023 року *Microsoft* пропонує[81] своїм клієнтам можливість зберігати та обробляти персональні дані у межах кордонів ЄС для своїх служб, таких як Microsoft 365, Azure, Power Platform та Dynamics 365. Це означає, що дані клієнтів будуть зберігатися та оброблятися в межах кордонів ЄС (EU Data Boundary)[82], що дозволяє скоротити потоки даних з Європи та забезпечити дотримання європейських законодавчих вимог щодо захисту персональних даних (GDPR).

Крім того, на наступних етапах програми *EU Data Boundary* передбачається розширення, щоб охопити зберігання та обробку додаткових категорій персональних даних, зокрема даних, які надаються під час отримання технічної підтримки. Програма включатиме псевдонімізацію даних і встановлення додаткових налаштувань для обмеження витоку даних за межі ЄС та ЄЗВТ. До середини 2024 року для захисту персональних даних в ході опрацювання запитів користувачів на технічну підтримку буде впроваджено безпечні віддалені робочі станції, що дозволить зберігати дані в межах *EU Data Boundary*.

Крім того, Microsoft планує збільшити кількість персоналу в регіоні EU Data Boundary та досліджує додаткові варіанти підтримки клієнтів для забезпечення того, щоб всі запити на підтримку оброблялися в Європі для початкового рішення проблеми. В цілому, ці кроки є додатковими заходами для забезпечення безпеки та конфіденційності даних клієнтів, що надають свої дані для технічної підтримки у межах EU Data Boundary.

81 Microsoft announces the phased rollout of the EU Data Boundary for the Microsoft Cloud begins January 1, 2023. https://blogs.microsoft.com/eupolicy/2022/12/15/eu-data-boundary-cloud-rollout/?culture=uk-ua&country=ua

82 Understanding the Microsoft EU Data Boundary Roadmap https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5dsVx



Локалізація даних: вплив на розвиток

Розвиток центрів обробки даних в України потребує значних довгострокових інвестицій, для яких потрібні гарантії їх повернення і сприятливі умови ведення бізнесу, включаючи застосування режиму «Дія.Сіті» (поєднання режиму оподаткування податком на додану вартість і податком на виведений капітал), а також підтримки у пріорітетному доступі до інфраструктури електропостачання.

Реалізувати такі стратегічні проекти можна буде за умови мінімізації ризиків, серед яких найбільш вагомим на цей час, принаймні психологічно, є ризик фізичного знищення внаслідок кінетичних атак в ході триваючого збройного конфлікту на території України. Компанії отримують значну цінність з використання даних, але більшість з них можуть досягти максимальної ефективності лише тоді, коли дані можуть вільно перетинати кордони.

Розширення локалізації даних на більшу кількість країн та типів даних є загрозою для розвитку відкритої та інноваційної глобальної цифрової економіки. В наш час, локалізація даних зменшує доступність та безпеку Інтернету, робить його складнішим та дорожчим, та обмежує інноваційні можливості.

Наприклад, звіт Організації економічного співробітництва та розвитку (ОЕСР) за 2018 рік показує, що цифровізація пов'язана з більшою відкритістю торгівлі та можливістю продажу товарів на більші ринки. Збільшення двостороннього цифрового зв›язку на 10 відсотків призводить до збільшення торгівлі послугами на 3,1 відсотка.

Але існує протилежна тенденція, про яку свідчать дослідження ITIF[83]. Збільшення індексу обмеження даних (DRI) країни на одиницю протягом п'ятирічного періоду призводить до зменшення її валової продукції на 7 відсотків, збільшення цін на товари та послуги на 1,5 відсотка та зниження продуктивності економіки на 2,9 відсотка.

Отже, **локалізація даних не сприятиме відновленню і розвитку економіки України**.

83 How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

Додатки

А. Угода про розміщення «Цифрової Амбасади» Естонії в Люксембурзі, 2017

Угода
між Естонською Республікою і Великим Герцогством Люксембург
щодо розміщення даних та інформаційних систем

Естонська Республіка та Велике Герцогство Люксембург, разом іменовані «Сторони»,

БЕРУЧИ до УВАГИ Меморандум про взаєморозуміння між Міністерством економіки та зв'язку Естонської Республіки та Міністерством мас-медіа та зв'язку Великого Герцогства Люксембург, підписаний 14 листопада 2016 року,

ОСКІЛЬКИ ця Угода відповідає духу Віденської конвенції про дипломатичні зносини,

БЕРУЧИ до УВАГИ Віденську конвенцію про дипломатичні зносини недостатньо для встановлення правової бази для розміщення даних та інформаційних систем,

ОСКІЛЬКИ цю Угоду укладено в рамках дипломатичних відносин між Естонською Республікою та Великим Герцогством Люксембург,

МАЮЧИ НАМІР визначити засоби для ефективного співробітництва між Сторонами та підтримки з боку Сторін, які є важливими для успішної та ефективної роботи приміщень, де розміщено естонські системи даних та інформації,

БАЖАЮЧИ укласти угоду, яка регулює правовий статус приміщень, де розміщено естонські системи даних та інформації, з необхідними гарантіями імунітету та привілеїв на основі чинного міжнародного та національного законодавства,

ПОГОДИЛИСЯ про таке:

Стаття 1

ВИЗНАЧЕННЯ

Для цілей цієї Угоди:

(a) «центр обробки даних» означає об'єкт, який використовується для розміщення даних та інформаційних систем, обладнання та ліцензій та пов'язаних компонентів, таких як телекомунікації та системи зберігання;

(b) «приміщення» означає виділений простір центру обробки даних, наданий Великим Герцогством Люксембург і призначений для розміщення естонських даних та інформаційних систем і обладнання;

(c) «системи даних та інформації» означає активи, які зберігаються на обладнанні Естонської Республіки в приміщеннях;

(d) «обладнання та ліцензії» означають активи, що належать Естонській Республіці та

використовуються для зберігання даних та інформаційних систем, що буде погоджено компетентними органами Сторін;

(e) «компетентні органи» означають Міністерство економіки та комунікацій для Естонської Республіки та «Державний центр інформаційних технологій» для Великого Герцогства Люксембург;

(f) «форс-мажорні обставини» означають будь-яку непередбачувану ситуацію або подію поза контролем Сторін, яка не була спричинена помилкою чи недбалістю з їхнього боку, і яка перешкоджає їм виконувати будь-які або всі свої зобов'язання за цією Угодою та будь-яким нормативним актом, що відносяться до нього.

Стаття 2

ФУНКЦІОНАЛЬНІСТЬ ПРИМІЩЕНЬ

(1) Приміщення повинні бути надані в повному робочому стані з метою розміщення естонських систем даних та інформації.

(2) Велике Герцогство Люксембург надає приміщення Естонській Республіці за вартість оренди, як зазначено в умовах, узгоджених компетентними органами Сторін.

(3) Велике Герцогство Люксембург надає доступ до приміщень уповноваженому представнику Естонської Республіки.

Стаття 3

НЕДОТОРКАННІСТЬ

(1) Приміщення є недоторканними і, таким чином, не підлягають обшуку, реквізиції, арешту чи виконавчим діям.

(2) Жодна посадова особа чи особа, яка виконує будь-які державні повноваження, будь то адміністративні, судові, військові чи поліцейські Люксембургу, не має права входити в приміщення без попереднього дозволу уповноваженого представника Естонської Республіки. Таке схвалення передбачається у випадку пожежі чи інших надзвичайних ситуацій, які потребують негайних захисних заходів і можуть становити загрозу для безпеки.

Стаття 4

ОХОРОНА ПРИМІЩЕНЬ

Велике Герцогство Люксембург вживає всіх необхідних заходів для захисту приміщень від будь-якого вторгнення або пошкодження на території Люксембургу. Заходи вважаються доцільними, якщо вони відповідають такому самому рівню захисту, як захист, запропонований Великому Герцогству Люксембург.

Стаття 5

ІМУНІТЕТ

Обладнання та ліцензії, необхідні для роботи центру обробки даних і розміщені на території Естонської Республіки, вважаються активами Естонської Республіки та користуються імунітетом від будь-якої форми судового процесу.

Стаття 6

АРХІВИ ТА КОМУНІКАЦІЇ

(1) Усі дані та інформаційні системи, що зберігаються Естонською Республікою в приміщеннях, вважаються архівами Естонської Республіки.

(2) Архіви приміщень є недоторканними і, таким чином, не підлягають обшуку, реквізиції, арешту чи виконавчим діям.

(3) Велике Герцогство Люксембург надає приміщенням такий самий режим, який надається дипломатичним представництвам щодо його офіційних повідомлень і передачі всіх документів.

(4) Естонська Республіка має право використовувати будь-який код і шифрування у своїх офіційних повідомленнях, а також відправляти та отримувати свої офіційні повідомлення дипломатичними кур'єрами, уповноваженими Естонською Республікою, і дипломатичну кореспонденцію.

(5) Жодна передача приміщень не підлягає цензурі чи будь-яким обмеженням, а також не може завдаватися шкоди її конфіденційному характеру. Цей захист поширюється, зокрема, на пристрої зберігання даних (наприклад, публікації, магнітні стрічки, оптичні диски, дискети, фотографії та фільми, а також візуальні або звукові записи).

(6) У разі форс-мажорних обставин, що призводять до повного або часткового припинення зв'язку, приміщення мають такий самий пріоритет, як і дипломатичні представництва.

Стаття 7

СУМІСНІСТЬ З МІЖНАРОДНИМ ПРАВОМ

Приміщення не можна використовувати будь-яким способом, несумісним з цілями, викладеними в цій Угоді або іншими нормами міжнародного права.

Стаття 8

ЗАСТОСОВНЕ ПРАВО ТА ВИРІШЕННЯ СПОРІВ

(1) Ця Угода регулюється та тлумачиться згідно з міжнародним правом і правом Європейського Союзу, доповненим, де це застосовно, законами та правилами Великого Герцогства Люксембург.

(2) Будь-який спір, що виникає між Сторонами внаслідок тлумачення або застосування цієї Угоди, яка не врегульована шляхом переговорів або іншим узгодженим способом врегулювання, передається для остаточного вирішення до арбітражного суду з трьох арбітрів, який формується для кожного окремого випадку таким чином. Протягом двох місяців після отримання запиту на арбітраж кожна Сторона призначає одного члена суду. Два члени, призначені таким чином потім обирає третього арбітра, який не є громадянином жодної зі Сторін. Цей третій арбітр є головою трибуналу.

(3) Якщо протягом трьох місяців від дати повідомлення про запит про арбітраж не було зроблено необхідних призначень, будь-яка зі Сторін може, за відсутності будь-якої іншої угоди, запросити Голову Міжнародного Суду ООН зробити необхідні призначення. Якщо Президент є громадянином будь-якої зі Сторін або якщо він чи вона не можуть виконувати зазначену функцію, Віце-президенту запрошується зробити необхідні призначення. Якщо Віце-президент є громадянином будь-якої зі Сторін або якщо він або вона також не можуть виконувати зазначену функцію, наступний за старшинством член Міжнародного Суду, який не є громадянином Естонії чи Люксембургу, запрошується зробити необхідні призначення.

(4) Рішення трибуналу є остаточними та обов'язковими. Трибунал ухвалює власні правила процедури.

(5) Витрати суду розподіляються порівну між Сторонами, якщо суд не вирішить інакше.

Стаття 9

ПОПРАВКИ

До цієї Угоди можуть бути внесені зміни за взаємною письмовою згодою Сторін. Кожна Сторона повідомляє іншу, як тільки її конституційні вимоги, необхідні для набрання чинності поправками, будуть виконані. Зміни набувають чинності через тридцять днів після останнього такого повідомлення.

Стаття 10

НАБРАННЯ ЧИННОСТІ ТА ПРИПИНЕННЯ

(1) Ця Угода набуває чинності, коли Сторони повідомлять одна одну про виконання відповідних конституційних вимог, необхідних для набрання чинності цією Угодою. Угода набирає чинності через тридцять днів після отримання останнього такого повідомлення.

(2) Естонська Республіка повідомляє дипломатичними каналами Велике Герцогство Люксембург про свого уповноваженого представника для виконання цієї Угоди та будь-яких наступних поправок до неї.

(3) Будь-яка Сторона може припинити дію цієї Угоди шляхом письмового повідомлення іншій Стороні. Розірвання набуває чинності через 24 місяці після дати повідомлення.

(4) Після припинення дії Угоди архіви, обладнання та ліцензії Естонської Республіки будуть передані лише уповноваженому представнику Естонської Республіки. Якщо неможливо ідентифікувати уповноваженого представника Естонської Республіки, Велике Герцогство Люксембург розглядатиме архіви, обладнання та ліцензії Естонської Республіки з тим самим рівнем захисту, що й архіви Великого Герцогства Люксембург і передає їх лише законному представнику Естонської Республіки.

Вчинено в Люксембурзі 20 дня червня місяця 2017 року в двох примірниках англійською мовою.

За Естонську Республіку	За Велике Герцогство Люксембург
Юрій РАТАС Прем›єр-міністр Естонської Республіки	Ксав'є БЕТТЕЛЬ Прем›єр-міністр Великого Герцогства Люксембург

B. Зразок форми DPIA для оцінки впливу на захист персональних даних, Управління інформаційного комісара Великої Британії

Зразок шаблону DPIA

Цей шаблон є прикладом того, як Ви можете записати процес і результат DPIA. Він відповідає процесу, викладеному в наших вказівках DPIA, і його слід читати разом із цими вказівками та Критеріями прийнятного DPIA, викладеними в європейських рекомендаціях щодо DPIA.

Ви повинні почати заповнювати шаблон на початку будь-якого великого проекту, що передбачає використання персональних даних, або якщо Ви вносите значні зміни в існуючий процес. Кінцеві результати повинні бути включені назад у Ваш план проекту.

Надсилання даних контролера	
Ім'я контролера	
Предмет/назва DPO	
Ім›я контактної особи контролера/DPO (видалити як потрібно)	

Крок 1: Визначте потребу в DPIA
Загально поясніть, на що спрямований проект і який тип обробки він передбачає. Вам може бути корисним посилання або посилання на інші документи, такі як проектна пропозиція. Підсумуйте, чому Ви визначили потребу в DPIA.

Крок 2: Опишіть обробку
Опишіть характер обробки: як Ви будете збирати, використовувати, зберігати та видаляти дані? Яке джерело даних? Чи будете Ви ділитися даними з кимось? Вам може бути корисно звернутися до блок-схеми або іншого способу опису потоків даних. Які типи обробки, визначені як високоризикові, задіяні?

Опишіть обсяг обробки: який характер даних, і чи включають вони дані про особливу категорію чи кримінальні правопорушення? Скільки даних Ви будете збирати та використовувати? Як часто? Як довго Ви будете це зберігати? Скільки осіб може постраждати? Яку географічну територію він охоплює?

Опишіть контекст обробки: який характер Ваших стосунків з людьми? Наскільки вони матимуть контроль? Чи очікують вони, що Ви будете використовувати їхні дані таким чином? Чи включають вони дітей чи інші вразливі групи? Чи є попередні занепокоєння щодо такого типу обробки чи недоліків безпеки? Який поточний стан технологій у цій галузі? Чи є якісь поточні проблеми, що викликають занепокоєння суспільства, які Ви повинні враховувати? Чи прийняли Ви будь-який затверджений кодекс поведінки або схему сертифікації (якщо їх буде затверджено)?

Опишіть цілі обробки: чого Ви хочете досягти? Який передбачуваний вплив на окремих людей? Які переваги обробки – для Вас і ширше?

Крок 3: Процес консультації

Подумайте, як консультуватися з відповідними зацікавленими сторонами: опишіть, коли і як Ви будете шукати думки окремих людей – або обґрунтуйте, чому це робити недоцільно. Кого ще Вам потрібно залучити до Вашої організації? Вам потрібно попросити своїх процесорів допомогти? Чи плануєте Ви консультуватися з експертами з інформаційної безпеки чи будь-якими іншими експертами?

Крок 4: Оцініть необхідність і пропорційність

Опишіть заходи відповідності та пропорційності, зокрема: яка Ваша правова основа для обробки? Чи справді обробка досягає Вашої мети? Чи є інший спосіб досягти такого ж результату? Як запобігти розповзанню функції? Як Ви забезпечите якість даних і мінімізацію даних? Яку інформацію Ви надасте особам? Як Ви допоможете відстояти їхні права? Які заходи Ви вживаєте, щоб забезпечити відповідність процесорів? Як Ви захищаєте будь-яку міжнародну передачу даних?

Крок 5: Визначте та оцініть ризики			
Опишіть джерело ризику та характер потенційного впливу на осіб. За потреби включіть пов'язану відповідність і корпоративні ризики.	Імовірність заподіяння шкоди	Тяжкість шкоди	Загальний ризик
	Віддалений, можливий або ймовірний	Мінімальний, значний або серйозний	Низький, середній або високий

Крок 6: Визначте заходи для зменшення ризику				
Визначте додаткові заходи, які Ви можете вжити для зменшення або усунення ризиків, визначених як середній або високий ризик на кроці 5				
Ризик	Варіанти зменшення або усунення ризику	Вплив на ризик	Залишковий ризик	Захід затверджено
		Ліквідовано зменшено прийнято	Низький середній високий	Так ні

Крок 7: Підпишіться та запишіть результати		
Пункт	**Ім'я/посада/дата**	**Примітки**
Заходи затверджені:		Інтегруйте дії назад у план проекту з датою та відповідальними за виконання
Залишкові ризики затверджені:		Якщо Ви приймаєте будь-який залишковий високий ризик, проконсультуйтеся з ICO, перш ніж продовжувати
Надані консультації DPO:		DPO має порадити щодо відповідності, кроку 6 заходів і чи можна продовжити обробку
Резюме порад DPO:		
Порада DPO прийнята або відхилена:		У разі відхилення ви повинні пояснити причини
Коментарі:		
Відповіді на консультацію перевірив:		Якщо ваше рішення розходиться з поглядами окремих осіб, ви повинні пояснити свої причини
Коментарі:		
Цей DPIA буде розглядатися:		DPO також має перевірити постійне дотримання DPIA

HQ 2011 Crystal Drive | Arlington, VA 22202 | USA
www.IFES.org