

Господарське право, господарське процесуальне право

УДК 346.7

Слюсаренко Віталій Анатолійович

*аспірант кафедри цивільного,
господарського та екологічного права
Національного технічного університету «Дніпровська політехніка»*

Sliusarenko Vitalii

*Postgraduate of the Department of Civil,
Economic and Environmental Law
Dnipro University of Technology*

**ПРАВОВЕ РЕГУЛЮВАННЯ ХМАРНИХ ПОСЛУГ В УКРАЇНІ:
ВІД РАМКОВОГО ЗАКОНУ ДО ФОРМУВАННЯ МОДЕЛІ
ЦИФРОВОГО СУВЕРЕНІТЕТУ
LEGAL REGULATION OF CLOUD SERVICES IN UKRAINE:
FROM FRAMEWORK LAW TO THE FORMATION OF A DIGITAL
SOVEREIGNTY MODEL**

***Анотація.** Вступ. Цифрова трансформація сфер публічного управління та господарських відносин супроводжується активним упровадженням хмарних технологій, які забезпечують ефективне використання інформаційних ресурсів, підвищують гнучкість управлінських механізмів і сприяють безперервності функціонування критично важливих електронних сервісів. В умовах воєнного стану особливої актуальності набувають питання належного правового регулювання, орієнтованого на гарантування кіберстійкості та захисту державних і корпоративних інформаційних систем. У статті розглянуто правову природу хмарних послуг, визначено тенденції їх розвитку та особливості законодавчого регулювання. Акцент зроблено на проблемних*

правових аспектах застосування цих технологій та необхідності подальшого вдосконалення нормативно-правової бази з метою забезпечення балансу між потребами держави, бізнесу й суспільства в умовах посилення глобальних безпекових викликів.

Мета. Метою дослідження є проаналізувати ефективність запроваджених законодавчих новацій у сфері хмарних послуг, виявити проблемні аспекти їх застосування та визначити основні подальші напрямки формування державної політики, здатної гарантувати кіберстійкість, правову визначеність і цифровий суверенітет.

Матеріали і методи. Матеріалами дослідження є нормативно-правові акти України, що регулюють сферу хмарних послуг, зокрема Закон України «Про хмарні послуги», постанови Кабінету Міністрів України та інші підзаконні нормативні акти; рішення та роз'яснення профільних регуляторних органів, зокрема Національного банку України, Національної комісії з цінних паперів та фондового ринку, Міністерства цифрової трансформації України, які визначають особливості застосування хмарних технологій у період воєнного стану; міжнародні регуляторні документи, що встановлюють правові засади функціонування ринку хмарних; наукові праці вітчизняних та зарубіжних дослідників, присвячені проблематиці правового регулювання цифрової економіки та інформаційної безпеки. У процесі дослідження використано комплекс загальнонаукових і спеціально-юридичних методів. Системний аналіз застосовано для виявлення взаємозв'язків між правовими нормами, що регулюють сферу хмарних технологій. Формально-юридичний метод дозволив здійснити тлумачення правових норм та з'ясувати їхнє практичне значення. Метод правового моделювання застосовано для визначення перспективних напрямів удосконалення нормативно-правової бази у сфері хмарних послуг та формулювання висновків дослідження.

Результати. Дослідження засвідчило, що в Україні триває активне формування засад правового регулювання хмарних послуг. Прийняття Закону України «Про хмарні послуги» та його розвиток у підзаконних нормативних актах стали відправною точкою для систематизації правовідносин у цій сфері. Аналіз правозастосовної практики воєнного часу та новел нормативного регулювання показав, що державна політика орієнтується насамперед на забезпечення кіберстійкості та захист критичних інформаційних ресурсів. Дозволи на використання іноземних хмарних середовищ у країнах ЄС, Великій Британії, США та Канаді стали вимушеною реакцією на загрозу фізичного знищення українських дата-центрів. Водночас приклад розгортання національних рішень, зокрема платформи «Дія» на базі приватних українських дата-центрів, підтвердив перспективність моделі «суверенної хмари», спрямованої на локалізацію даних і мінімізацію залежності від іноземних провайдерів. Встановлено, що чинна нормативно-правова база має рамковий характер і потребує подальшої конкретизації через впровадження підзаконних актів та адаптацію до міжнародних стандартів інформаційної безпеки. При цьому тенденції розвитку українського ринку свідчать про посилення ролі приватних ініціатив у формуванні національної хмарної інфраструктури, що в поєднанні з державним регулюванням створює передумови для становлення моделі цифрового суверенітету України.

Перспективи. У подальших наукових дослідженнях пропонується зосередити увагу на деталізації механізмів імплементації Закону України «Про хмарні послуги», на аналізі правових аспектів формування національної хмарної інфраструктури та на оцінці її здатності забезпечувати кіберстійкість і захист критичних даних. Дослідження в напрямку адаптації нормативної бази до міжнародних стандартів інформаційної безпеки дозволить сприяти зміцненню цифрового

суверенітету України та підвищити конкурентоспроможність українського ІТ-сектору.

Ключові слова: хмарні послуги, цифрова трансформація, хмарний суверенітет, кіберстійкість, правове регулювання, воєнний стан, державна політика.

Summary. *Introduction. The digital transformation of public administration and economic relations is accompanied by the active implementation of cloud technologies, which ensure the effective use of information resources, increase the flexibility of management mechanisms, and contribute to the continuity of critical electronic services. In the context of martial law, issues of proper legal regulation, aimed at guaranteeing cyber resilience and the protection of state and corporate information systems, become particularly relevant. The article examines the legal nature of cloud services, identifies their development trends, and the peculiarities of legislative regulation. Emphasis is placed on the problematic legal aspects of applying these technologies and the need for further improvement of the regulatory framework to ensure a balance between the needs of the state, business, and society in the face of increasing global security challenges.*

Purpose. *The purpose of the research is to analyse the effectiveness of implemented legislative innovations in the field of cloud services, identify problematic aspects of their application, and determine the main future directions for forming state policy capable of guaranteeing cyber resilience, legal certainty, and digital sovereignty.*

Materials and methods. *The research materials include regulatory acts of Ukraine governing the field of cloud services, in particular the Law of Ukraine "On Cloud Services", resolutions of the Cabinet of Ministers of Ukraine, and other subordinate regulatory acts; decisions and clarifications of relevant regulatory bodies, including the National Bank of Ukraine, the National*

Securities and Stock Market Commission, the Ministry of Digital Transformation of Ukraine, which define the peculiarities of applying cloud technologies during martial law; international regulatory documents establishing the legal framework for the functioning of the cloud services market in the EU; scientific works of domestic and foreign researchers dedicated to the problems of legal regulation of the digital economy and information security. The study used a complex of general scientific and special legal methods. System analysis was applied to identify the interconnections between legal norms regulating the field of cloud technologies. The formal legal method allowed for the interpretation of legal norms and clarification of their practical significance. The method of legal modelling was used to determine promising directions for improving the regulatory framework in the field of cloud services and to formulate the research conclusions.

Results. The study showed that the active formation of the legal framework for cloud services is ongoing in Ukraine. The adoption of the Law of Ukraine "On Cloud Services" and its development in subordinate regulatory acts became the starting point for systematising legal relations in this area. The analysis of wartime law enforcement practice and legislative innovations showed that state policy is primarily focused on ensuring cyber resilience and protecting critical information resources. Permissions to use foreign cloud environments in EU countries, Great Britain, the USA, and Canada became a forced reaction to the threat of physical destruction of Ukrainian data centres. At the same time, the example of deploying national solutions, in particular the "Diia" platform based on private Ukrainian data centres, confirmed the prospects of the "sovereign cloud" model, aimed at data localisation and minimising dependence on foreign providers. It was established that the current regulatory framework is of a framework nature and requires further concretisation through the implementation of subordinate acts and adaptation to international information security standards. At the same time, the development trends of the Ukrainian market indicate an increasing role of private initiatives in forming the national cloud

infrastructure, which, in combination with state regulation, creates prerequisites for the establishment of Ukraine's digital sovereignty model.

Discussion. Future scientific research is proposed to focus on detailing the mechanisms for implementing the Law of Ukraine "On Cloud Services", on analysing the legal aspects of forming the national cloud infrastructure, and on assessing its ability to ensure cyber resilience and protect critical data. Research in the direction of adapting the regulatory framework to international information security standards will help strengthen Ukraine's digital sovereignty and increase the competitiveness of the Ukrainian IT sector.

Key words: *cloud services, digital transformation, cloud sovereignty, cyber resilience, legal regulation, martial law, state policy.*

Постановка проблеми. В умовах постійної глобальної цифрової трансформації інформаційні технології виступають визначальним чинником розвитку як економічних відносин, так і системи державного управління. Особливу роль у цьому контексті відіграють технології хмарних послуг, які забезпечують органам публічної влади та суб'єктам господарювання можливість користуватися віддаленими дата-центрами, програмними сервісами та обчислювальними потужностями, що надаються спеціалізованими провайдерами. Такий підхід дозволяє мінімізувати потребу у створенні та підтриманні власної технічної інфраструктури, зменшити витрати на її обслуговування та отримати доступ до ресурсів у режимі «на вимогу». Протягом останнього десятиліття хмарні технології сформувалися як один із найефективніших і найперспективніших механізмів зберігання й обробки даних, що зумовило активний інтерес до їх застосування як у приватному секторі, так і в діяльності органів державної влади. Водночас розвиток цих технологій створює нові виклики для правової системи, яка має забезпечити належний рівень регулювання та захисту прав учасників відповідних правовідносин. Складність правового

регулювання у сфері хмарних послуг зумовлена міжгалузевим характером відповідних правовідносин, що охоплюють норми господарського, цивільного та інформаційного права, а також інститути захисту персональних даних і публічних закупівель. Виявлення наявних прогалин і подальший розвиток нормативного забезпечення цієї сфери набувають особливого значення в умовах воєнного стану, коли зростає потреба в безперебійному функціонуванні критичної інфраструктури, стабільності фінансової системи та належному захисті державних інформаційних реєстрів.

Аналіз останніх досліджень і публікацій. Питання розвитку та правового регулювання хмарних технологій активно досліджуються як у вітчизняній, так і в міжнародній науковій літературі. У роботі І. Надточія, І. Крамаренка та Н. Гришиної хмарні сервіси розглядаються як інструмент підвищення рівня фінансово-економічної безпеки підприємств та вдосконалення окремих операційних процесів у сучасних умовах цифровізації [1]. В. Кулик і М. Любимов зосередили увагу на аналізі можливостей, ризиків і перспектив застосування хмарних технологій у сфері бухгалтерського обліку суб'єктів господарювання [2]. У дослідженні О. Добровіцької та Ю. Лучко розглянуто специфіку застосування хмарних технологій у сфері вищої освіти, при цьому підкреслено їх значення для модернізації освітнього середовища та підвищення ефективності навчального процесу [3]. Схожі аспекти висвітлено у дослідженні О. Стойки та Д. Матейчук, яке присвячене інтеграції цифрових технологій у вищій школі [4]. Окреме місце займають праці, що стосуються договірного регулювання. Так, Н. Давидова досліджує цивільно-правові особливості договорів у сфері надання SaaS-послуг (Software as a Service), підкреслюючи необхідність чіткого визначення прав та обов'язків сторін [5]. Економічні аспекти впровадження хмарних технологій в Україні досліджували І. Шевчук та Б. Депутат, які проаналізували тенденції розвитку ринку хмарних

сервісів, окреслили переваги для бізнес-структур і державного сектору, а також вказали на ризики та необхідність нормативного врегулювання їх застосування [6]. У міжнародному науковому дискурсі переважає інтерес до проблем безпеки хмарних рішень, транскордонної передачі даних і захисту персональної інформації. Європейські дослідники приділяють значну увагу впровадженню базових регуляторних актів ЄС у сфері цифрової економіки, зокрема Регламенту про гармонізовані правила справедливого доступу до даних та їх використання (Data Act), який набув чинності 11 січня 2024 року та почав застосовуватися з 12 вересня 2025 року, а також Акта про цифрові ринки (Digital Markets Act) [7]. Ці документи визначають засади справедливого доступу до даних, забезпечують конкурентність цифрових ринків і сприяють розвитку інтероперабельності хмарних сервісів.

Постановка завдання. Оцінка ефективності чинного правового регулювання хмарних послуг в Україні та дослідження особливостей формування державної політики у сфері хмарних технологій як елемента цифрової трансформації й забезпечення інформаційної безпеки держави та бізнесу.

Виклад основного матеріалу. У сучасних умовах стратегія сталого розвитку провідних національних економік безпосередньо пов'язується з їхнім домінуванням у сфері наукових досліджень і технологічних розробок, активним продукуванням нових знань, формуванням високотехнологічних галузей виробництва та масовим упровадженням інноваційних рішень. Науково-технічний потенціал держави розглядається не лише як фундаментальний чинник економічного зростання та досягнення конкурентних переваг, але й як інструмент забезпечення національної безпеки, збереження державного суверенітету та підвищення рівня конкурентоспроможності у глобалізованому світі. Україна послідовно орієнтує свою державну політику на інтеграцію технологічних інновацій у ключові сфери економічної діяльності та державного управління.

Пріоритети державної політики у сфері інноваційної діяльності відображені у Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року, схваленій розпорядженням Кабінету Міністрів України та доповненій операційним планом заходів на 2025 – 2027 роки [8]. Важливу роль у цьому процесі відіграє Міністерство цифрової трансформації України, яке виконує функції центрального органу в сфері формування та реалізації державної політики з питань цифровізації, розвитку цифрової економіки, інноваційних технологій, електронної комерції, ІТ-індустрії, а також у сфері хмарних послуг [9]. Комплексність і системність відповідних заходів сприяють поступовому зростанню національного ІТ-сектору та розширенню кола суб'єктів господарювання, залучених до цифрової економіки. Очікується, що процес цифрової трансформації у найближчій перспективі охопить усі аспекти соціально-економічного життя більшості держав, оскільки формування інноваційно-інформаційного суспільства неможливе без домінування цифрової економіки як ключового елемента розвитку. Запровадження новітніх інформаційних технологій зумовлює суттєві зміни у правовому та соціальному середовищі, сприяючи підвищенню якості послуг, ефективності управління та продуктивності праці [10, с. 68].

У цьому контексті особливого значення набуває розвиток віддалених хмарних послуг як технологічної основи цифрової трансформації, що потребує належного правового врегулювання та інтеграції в правове поле України.

Важливим каталізатором активізації державної політики у сфері хмарних технологій стали надзвичайні безпекові обставини, пов'язані з воєнним станом. В умовах війни питання забезпечення кіберстійкості, захисту критично важливих державних інформаційних систем та збереження безперервності функціонування державних електронних сервісів набули особливої актуальності. Саме безпековий вимір сьогодні

визначає головні напрями правового регулювання – від локалізації даних і запровадження вимог до інфраструктури постачальників до вироблення національних стратегій цифрової безпеки та міжнародного співробітництва у сфері захисту хмарних сервісів.

Сучасна українська правова політика у сфері цифровізації характеризується поступовим формуванням комплексного публічно-правового механізму регулювання відносин, що виникають у процесі надання та використання хмарних послуг. Важливим кроком у цьому напрямі стало ухвалення Закону України «Про хмарні послуги», який заклав базові принципи функціонування ринку та визначив ключові вимоги у відносинах типу business-to-government (B2G), тобто у взаємодії постачальників послуг із державними органами та інституціями [11]. Цей закон не лише створив основу для правової визначеності у сфері хмарних технологій, а й підкреслив необхідність запровадження підвищених стандартів безпеки та надійності в роботі з державними інформаційними ресурсами.

Закон України «Про хмарні послуги» від 17 лютого 2022 року № 2075-IX, що набрав чинності 16 вересня 2022 року, спрямований на формування правових умов для належної обробки та захисту даних у процесі використання технологій хмарних обчислень. Його ухвалення мало на меті забезпечення можливостей для впровадження сучасних інформаційних технологій у діяльність органів державної влади, підвищення ефективності управління та раціонального використання державних ресурсів. Нормативний акт визначає коло правовідносин, що виникають у сфері надання та використання хмарних послуг, а також закріплює специфіку їх застосування органами державної влади, органами місцевого самоврядування, військовими формуваннями, створеними відповідно до законодавства України, державними підприємствами, установами й організаціями, суб'єктами владних повноважень та іншими

інституціями, яким делеговано виконання таких повноважень. Закон України «Про хмарні послуги» закріплює рамкове правове регулювання у сфері хмарних технологій, визначаючи базові дефініції та засади їх функціонування. Зокрема, у законі розкриваються ключові поняття, серед яких «хмарні обчислення», «хмарні послуги», «надавач хмарних послуг», «користувач хмарних послуг», «хмарні ресурси» та «центр обробки даних (ЦОД)». Документ встановлює класифікацію видів хмарних послуг і регламентує особливості їх використання, окреслює коло учасників відповідних правовідносин, визначає засади державного управління та регулювання в цій сфері, а також компетенцію регулятора комунікаційних послуг. Важливе значення надано вимогам до постачальників хмарних сервісів та операторів центрів обробки даних, у тому числі щодо включення до офіційного переліку надавачів таких послуг. Окремі положення закону присвячено врегулюванню порядку надання хмарних сервісів, пов'язаних із обробкою державних інформаційних ресурсів або інформації з обмеженим доступом, визначенню правил обробки персональних даних у хмарних середовищах, а також встановленню вимог до захисту інформації при наданні відповідних послуг. Окремий блок норм стосується міжнародного співробітництва, що має сприяти інтеграції України у світовий ринок хмарних технологій і підвищенню рівня інформаційної безпеки [11].

Таким чином, законодавець прагне забезпечити баланс між інноваційним розвитком ринку хмарних сервісів та належним рівнем захисту прав учасників правовідносин, безпеки даних і державних інтересів.

Відповідно до законодавчого визначення хмарна послуга трактується як діяльність з надання хмарних ресурсів за допомогою технологій хмарних обчислень, що забезпечує користувачу можливість віддаленого доступу до відповідної інфраструктури через електронні комунікаційні мережі. Законодавець виокремлює декілька основних різновидів таких послуг: інфраструктура як послуга (Infrastructure as a

Service, IaaS), яка полягає в наданні користувачам обчислювальних ресурсів, систем зберігання даних та електронних комунікаційних мереж; платформа як послуга (Platform as a Service, PaaS), що забезпечує доступ користувачів не лише до інфраструктури, а й до спеціалізованих програмних платформ, необхідних для розроблення та експлуатації інформаційних систем; програмне забезпечення як послуга (Software as a Service, SaaS), під якою слід розуміти надання доступу до прикладних програмних продуктів через онлайн-сервіси або спеціалізовані клієнтські додатки; окремо визначено категорію безпека як послуга (Security as a Service, SECaaS), яка передбачає надання користувачу послуг із кіберзахисту із застосуванням хмарних ресурсів. Крім перелічених, до хмарних можуть належати й інші послуги, що відповідають загальному визначенню та передбачають використання моделей хмарних обчислень [11].

Залежно від моделі розгортання інфраструктури хмарні послуги можуть надаватися на основі приватної, колективної, публічної або гібридної хмари, яка поєднує ознаки двох чи більше зазначених типів. Прогноз компанії Gartner свідчить, що до 2027 року більшість організацій застосовуватимуть так звані галузеві хмарні рішення, які поєднують у собі елементи трьох базових моделей хмарних сервісів (IaaS, PaaS, SaaS) [12].

Можемо констатувати, що прийняття базового закону стало відправною точкою для поетапної еволюції правового поля, орієнтованої на розбудову ринку хмарних сервісів в Україні та створення належних умов для залучення міжнародних постачальників. У сучасних умовах саме питання кібербезпеки значною мірою визначає напрями державної політики у сфері цифрової трансформації, будучи одним із ключових елементів системи національної безпеки. Для України, яка протистоїть збройній агресії, ця проблема постає особливо гостро, оскільки критична інфраструктура, державні реєстри, електронні архіви та комунікаційні

мережі постійно перебувають під ризиком суттєвого пошкодження чи знищення. З метою мінімізації ризиків блокування державних інформаційних систем і порушення діяльності інституцій уряд України ухвалив комплекс важливих стратегічних заходів. Вони стосуються перенесення центрів обробки даних за межі країни, активного впровадження хмарних технологій та створення надійних механізмів захисту інформації. Ці заходи стимулюють подальший розвиток українського ринку хмарних послуг, що відкриває додаткові можливості для глобальних провайдерів, таких як Amazon, Google, Microsoft тощо. Разом із тим законодавство встановлює для іноземних і вітчизняних надавачів низку регуляторних вимог та стандартів, спрямованих на гарантування безпеки користувачів та захист національних інтересів.

Нинішній перехідний етап відзначається низкою нормативних новацій, ухвалення яких було відтерміновано у зв'язку з початком повномасштабного вторгнення. Внаслідок військової агресії проти України правова процедура офіційної реєстрації провайдерів хмарних послуг певний час залишалася призупиненою, що ускладнювало завершення відповідних процедур через відсутність затверджених форматів документів і конкретизованих вимог. Вирішення цієї проблеми відбулося 11 лютого 2025 року, коли Кабінет Міністрів України ухвалив постанову № 154 «Деякі питання надання та використання хмарних сервісів та/або послуг центрів обробки даних». Зазначений акт ліквідував попередні правові прогалини, запровадив перехідний період та унормував порядок реєстрації постачальників хмарних послуг.

Прийнята постанова Кабінету Міністрів України була ухвалена на виконання Закону України «Про хмарні послуги» та врегулювала ключові питання функціонування ринку. Документ визначив порядок надання послуг, пов'язаних з обробкою державних інформаційних ресурсів та інформації з обмеженим доступом, встановив вимоги до постачальників і

унормував правила формування й використання електронних каталогів послуг. Важливим елементом стала поява типового договору про надання послуг публічним користувачам та операторам критичної інфраструктури. Так, надання послуг із обробки державних інформаційних ресурсів чи інформації з обмеженим доступом повинно здійснюватися на договірній основі з обов'язковим підтвердженням відповідності постачальника вимогам інформаційної безпеки та безперервності роботи. Вимоги до постачальників охоплюють технічні, організаційні та безпекові заходи, включаючи впровадження систем управління інформаційною безпекою або комплексних систем захисту інформації, проходження експертизи та підтвердження відповідності міжнародним і національним стандартам (ISO/IEC 27001, ISO/IEC 27018, ДСТУ ISO/IEC 27001:2023). Необхідною умовою є наявність документів про відповідність, політик з обробки персональних даних та підтвердження прав на використання інфраструктури. Запроваджено процедуру ведення електронних каталогів послуг, які публікуються державною мовою на сайтах провайдерів і містять інформацію про характеристики послуг, порядок захисту даних, розташування ресурсів, стандарти відповідності та відомості про постачальника. Каталоги використовуються публічними користувачами та операторами критичної інфраструктури під час планування закупівель відповідно до Закону України «Про публічні закупівлі». Типовий договір закріплює умови доступу до послуг, порядок розрахунків, права та обов'язки сторін. Він передбачає обов'язок постачальника негайно інформувати користувача та урядову команду реагування на комп'ютерні надзвичайні події CERT-UA про кіберінциденти, а також встановлює відповідальність у вигляді штрафних санкцій у разі неналежної якості чи порушення строків надання послуг. Дострокове розірвання можливе за взаємною згодою сторін, у разі невиконання умов договору або втрати

чинності документів, що підтверджують відповідність вимогам безпеки [13].

Варто зауважити, що прийняття та затвердження Типового договору про надання хмарних послуг і послуг центрів обробки даних для публічних користувачів та операторів критичної інфраструктури стало важливим етапом у розвитку правового регулювання в цій сфері та фактично зняло тривалі наукові дискусії щодо правової природи таких договорів у цивільному законодавстві. До цього моменту серед науковців не було єдності стосовно їх класифікації – частина авторів схилилася до того, що йдеться про договір надання послуг, тоді як інші вбачали ознаки договору оренди або договору зберігання. Такі підходи пояснювалися специфікою хмарних технологій, адже технічно вони полягають у наданні користувачу доступу до певних серверних потужностей для збереження інформації, що могло сприйматися як умовні оренда чи зберігання даних. Проте, як зазначає Є. Євлахова, саме договір про надання послуг найбільш адекватно відображає сутність цих правовідносин [14, с. 19–22]. Подібної позиції дотримується й Н. Давидова, яка акцентує на доцільності застосування моделі договору інформаційних послуг у сфері Software as a Service (SaaS) [5, с. 20–21].

Отже, нині законодавчо закріплено підхід, згідно з яким договір про надання послуг розглядається як найбільш універсальний правовий інструмент, здатний врахувати багатофункціональність та динаміку хмарних сервісів. Саме його гнучкість щодо предмета та умов надання дозволяє охопити широкий спектр відносин, які не можна вичерпно пояснити крізь призму інших класичних інститутів права.

Прийняття вказаної постанови відкрило можливість офіційної реєстрації постачальників хмарних послуг. На перехідний період, що триватиме до 31 грудня 2025 року, державним установам дозволено здійснювати закупівлю хмарних сервісів у компаній, які ще не пройшли

процедуру реєстрації. Водночас після завершення цього етапу реєстрація стане обов'язковою умовою для співпраці з органами державної влади та об'єктами критичної інфраструктури [13].

Відтак реєстрація в статусі надавача хмарних послуг відкриває доступ до співпраці з державними органами та об'єктами критичної інфраструктури, що буде стратегічною перевагою на українському ринку. Український ринок хмарних послуг динамічно формується. Він відкриває значні можливості для глобальних провайдерів, особливо з огляду на масштабну цифровізацію державного сектору та зростання ІТ-індустрії. Водночас ефективний вихід на цей ринок можливий за умови дотримання законодавчих вимог щодо реєстрації, кібербезпеки та надійності інфраструктури. Ті учасники ринку, які вчасно адаптуються до нових правил, отримають довгострокові конкурентні переваги та зможуть закріпитися на перспективному українському ринку хмарних сервісів.

Варто зауважити, що на формування державної політики України у сфері хмарних послуг істотно вплинули безпекові виклики, пов'язані з початком повномасштабного вторгнення у 2022 році. З огляду на критичне значення даних для функціонування державних органів і суспільних інститутів, воєнні дії створили пряму загрозу для збереження та безперервності роботи серверів, на яких зберігаються публічні бази, державні реєстри та службова інформація. При цьому на початок агресії Україна не мала достатньо розвиненої матеріальної та організаційної інфраструктури для захисту таких даних. Протягом багатьох років більшість державних реєстрів функціонували на власних технологічних майданчиках органів влади, які відповідали за їх адміністрування. Водночас через високу вартість модернізації та стрімкий розвиток інформаційних технологій державні центри обробки даних поступово застаріли й нині потребують комплексного оновлення [15].

Ці обставини зумовили прийняття ряду рішень, спрямованих на можливість використання закордонних хмарних сервісів. Так, постановою Національного банку України від 8 березня 2022 року № 42 було дозволено на період воєнного стану та протягом двох років після його завершення зберігати клієнтські дані, у тому числі ті, що містять банківську таємницю, у хмарних сервісах, розташованих у країнах ЄС, Великій Британії, США та Канаді [16]. Подібний підхід було закріплено й у сфері ринку капіталу, зокрема 4 серпня 2022 року Національна комісія з цінних паперів та фондового ринку дозволила депозитарним установам і Центральному депозитарію використовувати хмарні сервіси, розташовані в зазначених юрисдикціях [17]. Крім того, 30 грудня 2022 року Кабінет Міністрів України ухвалив постанову № 1500, якою врегульовано можливість розміщення державних інформаційних ресурсів за межами України. Йдеться про дані, що не містять відомостей, віднесених до державної таємниці чи службової інформації, які можуть зберігатися у закордонних хмарних середовищах за умови застосування криптографічного захисту та дотримання спеціальних процедур погодження із Службою безпеки України [18]. Надалі правове регулювання було уточнено й щодо найбільш чутливих категорій даних. Зокрема, змінами до Закону України «Про хмарні послуги» від 16 січня 2024 року № 3549-IX визначено, що в умовах воєнного стану дані, які становлять державну таємницю і належать Міністерству оборони України, Збройним Силам України та іншим військовим формуванням, можуть бути розміщені на хмарах, розташованих у державах-членах НАТО, за умови погодження відповідного рішення Міністром оборони та Генеральним штабом і негайного інформування профільного комітету Верховної Ради України [19].

Водночас у приватному секторі економіки також відбуваються зміни в стратегіях використання хмарних технологій. Показовим прикладом є досвід страхової компанії «ІНГО», яка після початку повномасштабної

війни зіткнулася з ризиками втрати даних та простоїв у роботі через перебої з електропостачанням. Щоб мінімізувати ці ризики, в жовтні 2022 року компанія запровадила гібридну модель ІТ-інфраструктури, розподіливши роботу між власним дата-центром та приватною хмарою, створеною оператором GigaCloud у Варшаві. Це дало змогу гарантувати безперервність бізнес-процесів навіть за умов воєнних загроз [20].

Поряд із цим простежується тенденція до переосмислення стратегій використання хмарних технологій, що безпосередньо пов'язано з необхідністю забезпечення цифрового суверенітету та мінімізації залежності від іноземних провайдерів. У 2025 році провідні українські хмарні провайдери – De Novo, GigaCloud та Датацентр «Парковий» – ініціювали створення альянсу, головною метою якого є розбудова національної хмарної інфраструктури. Ініціатива спрямована на формування умов для збереження критично важливих державних і корпоративних даних безпосередньо на території України, що дозволяє усунути ризики їх блокування, вилучення чи обмеження доступу внаслідок дії іноземного законодавства або геополітичних факторів. Учасники альянсу наголошують, що залежність від зовнішніх постачальників у сфері обробки даних може створювати загрози для національної безпеки, оскільки ключові інформаційні ресурси держави фактично перебувають поза межами її контролю. Актуальною проблемою є відсутність у більшості українських сервісів прямих договірних відносин із глобальними провайдерами (Amazon, Microsoft Azure тощо). Як правило, такі контракти укладаються через локальні компанії-посередники, що істотно підвищує ризик одностороннього припинення надання послуг з боку міжнародних гравців у будь-який момент. Подібна ситуація зумовлена тим, що правове регулювання діяльності глобальних провайдерів здійснюється відповідно до законодавства іноземних держав, насамперед США, і практично не враховує специфіку національної юрисдикції України. В умовах

нестабільної геополітичної ситуації це створює реальну загрозу для безперервності функціонування критичних цифрових сервісів. При цьому втрата доступу до даних несе ризик втрати ключових елементів національної цифрової екосистеми, зокрема пов'язаних не лише з хмарними провайдерами чи дата-центрами, а й із підготовкою кадрів, розвитком освітніх програм та інноваційних технологій [21].

У відповідь на зазначені виклики одним із ключових напрямів стала практична реалізація національних хмарних рішень, що дозволяють гарантувати збереження та захист даних у межах української юрисдикції. Показовим прикладом цього процесу є розгортання державної платформи «Дія» на базі дата-центрів українських хмарних провайдерів. Її інфраструктура реалізована за принципом Active-Active, що передбачає роботу в двох географічно розподілених приватних дата-центрах (GigaCloud та DeNovo), з'єднаних незалежними оптичними каналами зв'язку. Такий підхід забезпечує відмовостійкість, географічне резервування даних і відповідність вимогам інформаційної безпеки, які раніше досягалися здебільшого шляхом використання глобальних провайдерів рівня Amazon чи Microsoft [22].

Отже, для українських провайдерів хмарних послуг постає об'єктивна необхідність розбудови спільного сервісного простору, покликаного виконувати функцію єдиної точки доступу для державних органів, ІТ-компаній та розробників. Такий простір має забезпечувати надійну альтернативу західним хмарним платформам, гарантувати локальне зберігання даних і відповідність національним стандартам інформаційної безпеки, що в умовах воєнного стану й загострення глобальних кіберзагроз набуває стратегічного значення. У цьому контексті формування так званої «суверенної хмари» розглядається не лише як інструмент забезпечення інформаційної безпеки, а й як стратегічний напрям розвитку українського ІТ-сектору, здатний стимулювати інвестиції, сприяти технологічній

модернізації та формувати конкурентні переваги на глобальному ринку. Однак ефективне функціонування спільного сервісного простору неможливе без належного правового регулювання, яке визначає вимоги до провайдерів, порядок взаємодії з органами державної влади, стандарти кіберзахисту та механізми контролю за обробкою даних. Наявність комплексної нормативної бази – від рамкового Закону України «Про хмарні послуги» до підзаконних імплементаційних актів – забезпечує правову визначеність і створює умови для сталого розвитку ринку. Таким чином стратегія об'єднання вітчизняних провайдерів хмарних сервісів набуває особливого значення в умовах воєнного стану й може стати одним із ключових чинників у розбудові моделі цифрового суверенітету України.

Висновки. Загалом аналіз наукових праць та нормативних матеріалів дає підстави стверджувати, що Закон України «Про хмарні послуги» має рамковий характер, оскільки значною мірою його ефективність залежить від діяльності регулятора та від прийняття підзаконних актів, що деталізують механізми його реалізації. Водночас збройна агресія проти України виступила поштовхом до формування нових тенденцій у сфері розвитку хмарних технологій. Перед державою та бізнесом постала дилема: з одного боку – актуальною є потреба в збереженні «хмарного суверенітету» та забезпеченні належного контролю над державними інформаційними ресурсами, а з іншого – воєнні реалії висунули на перший план питання фізичного захисту даних, що нерідко вимагає їх розміщення на серверах за межами України. У результаті регулятори дозволили виведення певних категорій даних до хмарних середовищ у країнах НАТО та в інших державах із розвинутими інститутами кіберзахисту.

Аналіз досвіду практичного застосування хмарних сервісів в умовах воєнного стану та поточного нормативного регулювання відповідних правовідносин свідчить про поступове формування державної політики,

орієнтованої на гарантування кіберстійкості та захисту даних критично важливої інформаційної інфраструктури. Першочерговим завданням стає не лише гарантування безперервності роботи державних реєстрів та сервісів, а й створення умов для надійного захисту даних у випадках масованих кібератак чи фізичного знищення центрів обробки даних. Відтак подальший розвиток правового регулювання має будуватися на комплексному підході, який включає вдосконалення систем організації й менеджменту даних, розробку детальних планів кризового реагування, механізмів відновлення після інцидентів та чітке визначення відповідальності учасників ринку.

У довгостроковій перспективі поточна правозастосовна практика у сфері регулювання хмарних сервісів може стати орієнтиром як для України у процесі подальшого вдосконалення нормативного середовища, так і для інших держав, що стикаються з подібними викликами. В умовах зростання ролі цифрових даних у глобальній економіці та політичних процесах саме Україна здатна напрацювати унікальний досвід формування політики «хмарного суверенітету», заснованої на управлінні ризиками та врахуванні навіть найбільш несприятливих сценаріїв розвитку подій. Така політика має передбачати створення стандартів у сфері обробки та захисту даних, уніфікацію вимог до збереження критичної інформації, а також розширення міждержавної співпраці у питаннях кіберзахисту. В результаті можна очікувати поступове становлення національної моделі управління хмарними послугами, яка поєднуватиме принципи безпеки, суверенітету та технологічної інноваційності.

Ураховуючи складний і комплексний характер регуляторних процесів у сфері хмарних технологій, особливого значення набувають наукові дослідження, спрямовані на оцінку ефективності застосування чинних правових норм в умовах збройного конфлікту та загострення проблем кібербезпеки. Не менш значущим завданням є продовження досліджень у сфері публічного управління та цифрової інфраструктури,

зокрема щодо інтеграції хмарних сервісів у діяльність державних інформаційних систем. Це питання набуває особливої актуальності в умовах обмежених фінансових і технічних ресурсів, а також нагальної потреби модернізації державних центрів обробки даних. Окремим напрямом виступає вивчення міжнародного співробітництва та формування політики «хмарного суверенітету», що передбачає розробку узгоджених підходів між Україною та державами ЄС, НАТО й іншими країнами, які вже мають усталені практики у сфері транскордонної передачі даних і гарантування їх захисту. Розробка окреслених напрямів сприятиме не лише вдосконаленню національного законодавства України, а й створить підґрунтя для формування стандартів, здатних забезпечити оптимальний баланс між інноваційним розвитком, інформаційною безпекою та збереженням цифрового суверенітету держави при використанні хмарних технологій.

Література

1. Надточій І.І., Крамаренко І.С., Гришина Н.В. Хмарні технології як інструмент ефективного управління фінансово-економічною безпекою та HR-технологіями в умовах цифровізації. *Економічний простір*. 2024. № 190. С. 187–191. DOI: <https://doi.org/10.32782/2224-6282/190-34>

2. Кулик В.А., Любимов М.О. Можливості, загрози та перспективи використання "хмарних" технологій у бухгалтерському обліку. *Науковий вісник Полтавського університету економіки і торгівлі. Серія: Економічні науки*. 2019. № 2. С. 40–46. URL: http://nbuv.gov.ua/UJRN/Nvpushk_2019_2_7 (дата звернення: 15.09.2025).

3. Добровіцька О.О., Лучко Ю.І. Застосування хмарних технологій в освітньому процесі закладів вищої освіти. *Освіта та педагогічна наука*. 2023. № 2 (183). С. 62–70. URL: <https://dspace.luguniv.edu.ua/xmlui/handle/123456789/10682> (дата звернення: 15.09.2025).

4. Стойка О., Матейчук Д. Сучасні підходи до впровадження цифрових технологій в освітній процес ЗВО. *Актуальні питання гуманітарних наук*. 2023. Вип. 62, том 2. С. 297-301. URL: https://www.aphn-journal.in.ua/archive/62_2023/part_2/48.pdf (дата звернення: 15.09.2025).

5. Давидова Н.О. Цивільно-правове регулювання інформаційних відносин SaaS (Software as a Service). *Підприємництво, господарство і право*. 2021. № 6. С. 16–22. DOI: <https://doi.org/10.32849/2663-5313/2021.6.03>

6. Шевчук І.Б., Депутат Б.Я. Економічний аспект використання хмарних технологій у діяльності органів публічної влади та бізнес-структур. *Економіка та суспільство*. 2021. № 31. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/689> (дата звернення: 15.09.2025).

7. Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies. Centre on Regulation in Europe (CERRE), February 2024. URL: https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf (дата звернення: 15.09.2025).

8. Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року та затвердження операційного плану заходів з її реалізації у 2025–2027 роках: розпорядження Кабінету Міністрів України від 31.12.2024 № 1351-р. URL: <https://zakon.rada.gov.ua/laws/show/1351-2024-p#n466> (дата звернення: 15.09.2025).

9. Про Міністерство цифрової трансформації України: Положення затверджене постановою Кабінету Міністрів України від 18.09.2019 №856. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text> (дата звернення: 15.09.2025).

10. Череп А.В., Воронкова В.Г., Череп О.Г. Цифрова трансформація суспільства як необхідна умова його інноваційного розвитку. *Теорія і*

практика інтелектуальної власності. 2022. № 2. С. 68–72. URL: <http://uran.inprojournal.org/article/view/259745> (дата звернення: 15.09.2025).

11. Про хмарні послуги: Закон України від 17.02.2022 р. № 2075-IX. URL: <https://zakon.rada.gov.ua/laws/show/2075-20#Text> (дата звернення: 15.09.2025).

12. Gartner report shows AI and cloud a priority for 2023. SDxCentral. 2023. URL: <https://www.sdxcentral.com/analysis/gartner-report-shows-ai-and-cloud-a-priority-for-2023/> (дата звернення: 16.09.2025).

13. Деякі питання надання та використання хмарних сервісів та/або послуг центрів обробки даних: Постанова Кабінету Міністрів України від 11.02.2025 № 154. URL: <https://zakon.rada.gov.ua/laws/show/154-2025-%D0%BF#Text> (дата звернення: 16.09.2025).

14. Євлахова Е.Р. Істотні умови договорів про використання технологій хмарних обчислень. *Молодий вчений*. 2021. № 11 (99). С. 19–22. URL: <https://molodyivchenyi.ua/index.php/journal/article/view/2382/2368> (дата звернення: 16.09.2025).

15. Звіт за результатами аналітичного дослідження «Стан та перспективи розвитку державних електронних інформаційних ресурсів». USAID / UK aid проєкт «Прозорість та підзвітність у державному управлінні та послугах / TAPAS». 2020. URL: <https://tapas.org.ua/wp-content/uploads/2020/08/1530105013.pdf> (дата звернення: 16.09.2025).

16. Про використання банками хмарних послуг в умовах воєнного стану в Україні: Постанова Національного банку України від 08.03.2022 р. № 42. URL: <https://zakon.rada.gov.ua/laws/show/v0042500-22#Text> (дата звернення: 16.09.2025).

17. Про використання у період дії воєнного стану учасниками фондового ринку хмарних послуг та/або послуг центрів обробки даних: Рішення Національної комісії з цінних паперів та фондового ринку від

04.08.2022 № 1054. URL: <https://zakon.rada.gov.ua/rada/show/v1054863-22#Text> (дата звернення: 16.09.2025).

18. Деякі питання забезпечення функціонування державних інформаційних ресурсів: Постанова Кабінету Міністрів України від 30.12.2022 р. № 1500. URL: <https://zakon.rada.gov.ua/laws/show/1500-2022-p#Text> (дата звернення: 16.09.2025).

19. Про внесення змін до деяких законів України щодо удосконалення порядку обробки та використання даних у державних реєстрах для військового обліку та набуття статусу ветерана війни під час дії воєнного стану: Закон України від 16.01.2024 р. № 3549-IX. URL: <https://zakon.rada.gov.ua/laws/show/3549-20#Text> (дата звернення: 16.09.2025).

20. Як страхова компанія INGO перенесла інфраструктуру в хмару та унікає форс-мажорів. *GigaCloud.ua*. 2022. URL: <https://gigacloud.ua/cases/yak-strahova-kompaniya-ingo-perenesla-infrastrukturu-v-hmaru-ta-unykaye-fors-mazhoriv> (дата звернення: 16.09.2025).

21. «Уся податкова стоїть за кордоном». Українські хмарні провайдери побоюються: доступ до критичних держданих за кордоном може бути втрачений в будь-який момент. *DEV.ua*. 2025. URL: <https://dev.ua/news/dani-1745348018> (дата звернення: 16.09.2025).

22. "Дія" переїхала на відмовостійку інфраструктуру, до 2022 року планують добудувати державний дата-центр. *Інтерфакс-Україна*. 2021. URL: <https://interfax.com.ua/news/telecom/778223.html> (дата звернення: 16.09.2025).

References

1. Nadtochii I.I., Kramarenko I.S., Hryshyna N.V. Khmarni tekhnolohii yak instrument efektyvnoho upravlinnia finansovo-ekonomichnoiu bezpekoiu ta

HR-tekhnologiiamy v umovakh tsyfrovizatsii. Ekonomichnyi prostir. 2024. № 190. S. 187–191. DOI: <https://doi.org/10.32782/2224-6282/190-34>

2. Kulyk V.A., Liubymov M.O. Mozhlyvosti, zahrozy ta perspektyvy vykorystannia "khmarnykh" tekhnologii u bukhholderskomu obliku. Naukovyi visnyk Poltavskoho universytetu ekonomiky i torhivli. Seriya: Ekonomichni nauky. 2019. № 2. S. 40–46. URL: http://nbuv.gov.ua/UJRN/Nvpushk_2019_2_7

3. Dobrovitska O.O., Luchko Yu.I. Zastosuvannia khmarnykh tekhnologii v osvithomu protsesi zakladiv vyshchoi osvity. Osvita ta pedahohichna nauka. 2023. № 2 (183). S. 62–70. URL: <https://dspace.luguniv.edu.ua/xmlui/handle/123456789/10682>

4. Stoika O., Mateichuk D. Suchasni pidkhody do vprovadzhennia tsyfrovyykh tekhnologii v osvithii protses ZVO. Aktualni pytannia humanitarnykh nauk. 2023. Vyp. 62, tom 2. S. 297-301. URL: https://www.aphn-journal.in.ua/archive/62_2023/part_2/48.pdf

5. Davydova N.O. Tsyvilno-pravove rehuliuвання informatsiinykh vidnosyn SaaS (Software as a Service). Pidpryemnytstvo, hospodarstvo i pravo. 2021. № 6. S. 16–22. DOI: <https://doi.org/10.32849/2663-5313/2021.6.03>

6. Shevchuk I.B., Deputat B.Ia. Ekonomichnyi aspekt vykorystannia khmarnykh tekhnologii u diialnosti orhaniv publichnoi vlady ta biznes-struktur. Ekonomika ta suspilstvo. 2021. № 31. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/689>

7. Competition and Regulation of Cloud Computing Services: Economic Analysis and Review of EU Policies. Centre on Regulation in Europe (CERRE), February 2024. URL: https://cerre.eu/wp-content/uploads/2024/02/REPORT.CERRE_.FEB24.CLOUDS.pdf

8. Pro skhvalennia Stratehii tsyfrovoho rozvytku innovatsiinoi diialnosti Ukrainy na period do 2030 roku ta zatverdzhennia operatsiinoho planu zakhodiv z yii realizatsii u 2025–2027 rokakh: Rozporiadzhennia Kabinetu Ministriv

Ukrainy vid 31.12.2024 № 1351-r. URL:
<https://zakon.rada.gov.ua/laws/show/1351-2024-r#n466>

9. Pro Ministerstvo tsyfrovoi transformatsii Ukraïny: Polozhennia zatverdzhene postanovoiu Kabinetu Ministriv Ukraïny vid 18.09.2019 №856. URL: <https://zakon.rada.gov.ua/laws/show/856-2019-%D0%BF#Text>

10. Cherep A.V., Voronkova V.H., Cherep O.H. Tsyfrova transformatsiia suspilstva yak neobkhidna umova yoho innovatsiinoho rozvytku. Teoriia i praktyka intelektualnoi vlasnosti. 2022. № 2. S. 68–72. URL: <http://uran.inprojournal.org/article/view/259745>

11. Pro khmarni posluhy: Zakon Ukraïny vid 17.02.2022 r. № 2075-IX. URL: <https://zakon.rada.gov.ua/laws/show/2075-20#Text>

12. Gartner report shows AI and cloud a priority for 2023. SDxCentral. 2023. URL: <https://www.sdxcentral.com/analysis/gartner-report-shows-ai-and-cloud-a-priority-for-2023/>

13. Deiaki pytannia nadannia ta vykorystannia khmarnykh servisiv ta/abo posluh tsentriv obrobky danykh: postanova Kabinetu Ministriv Ukrainy vid 11.02.2025 № 154. URL: <https://zakon.rada.gov.ua/laws/show/154-2025-%D0%BF#Text>

14. Ievlakhova E.R. Istotni umovy dohovoriv pro vykorystannia tekhnolohiy khmarnykh obchyslen. Molodyy vchenyy. 2021. № 11 (99). S. 19–22. URL: <https://molodyivchenyi.ua/index.php/journal/article/view/2382/2368>



15. Zvit za rezultatamy analitychnoho doslidzhennia «Stan ta perspektyvy rozvytku derzhavnykh elektronnykh informatsiinykh resursiv». USAID / UK aid proiekt «Prozorist ta pidzvithnist u derzhavnomu upravlinni ta posluhakh / TAPAS». 2020. URL: <https://tapas.org.ua/wp-content/uploads/2020/08/1530105013.pdf>

16. Pro vykorystannia bankamy khmarnykh posluh v umovakh voiennoho stanu v Ukraini: Postanova Natsionalnoho banku Ukrainy vid 08.03.2022 r. № 42. URL: <https://zakon.rada.gov.ua/laws/show/v0042500-22#Text>

17. Pro vykorystannia u period dii voiennoho stanu uchasnykamy fondovoho rynku khmarnykh posluh ta/abo posluh tsentriv obrobky danykh: rishennia Natsionalnoi komisii z tsinnykh paperiv ta fondovoho rynku vid 04.08.2022 № 1054. URL: <https://zakon.rada.gov.ua/rada/show/v1054863-22#Text>

18. Deiaki pytannia zabezpechennia funktsionuvannia derzhavnykh informatsiinykh resursiv: Postanova Kabinetu Ministriv Ukrainy vid 30.12.2022 r. № 1500. URL: <https://zakon.rada.gov.ua/laws/show/1500-2022-p#Text>

19. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo udoskonalennia poriadku obrobky ta vykorystannia danykh u derzhavnykh reiestrach dlia viiskovoho obliku ta nabuttia statusu veterana viiny pid chas dii voiennoho stanu: Zakon Ukrainy vid 16.01.2024 r. № 3549-IX. URL: <https://zakon.rada.gov.ua/laws/show/3549-20#Text>

20. Iak strakhova kompaniia INGO perenesla infrastrukturu v khmaru ta unykaie fors-mazhoriv. GigaCloud.ua. 2022. URL: <https://gigacloud.ua/cases/yak-strahova-kompaniya-ingo-perenesla-infrastrukturu-v-hmaru-ta-unykaye-fors-mazhoriv>

21. «Usia podatкова stoit za kordonom». Ukrainski khmarni provaidery poboiiutsia: dostup do krytychnykh derzhdanykh za kordonom mozhe buty vtrachenyi v bud-yakyi moment. DEV.ua. 2025. URL: <https://dev.ua/news/dani-1745348018>

22. "Diia" pereikhala na vidmovostiiku infrastrukturu, do 2022 roku planuiut dobuduvaty derzhavnyi data-tsentr. Interfaks-Ukraina. 2021. URL: <https://interfax.com.ua/news/telecom/778223.html>