УДК 347
DOI https://doi.org/10.32782/chern.v1.2023.6

Е. Р. Євлахова
аспірантка кафедри цивільного права № 1
Національного юридичного університету
імені Ярослава Мудрого
orcid.org/0000-0002-7216-6582

ЗАГАЛЬНОТЕОРЕТИЧНІ ЗАСАДИ ЗАХИСТУ ПРАВ ТА ІНТЕРЕСІВ СУБ'ЄКТІВ ДОГОВІРНИХ ВІДНОСИН У СФЕРІ ТЕХНОЛОГІЙХ МАРНИХ ОБЧИСЛЕНЬ

Цифровізація світового господарства та всіх процесів, що відбуваються у світі, вже давно почала крокувати вперед дуже швидкими темпами. У країнах всього світу вже давно прийшли до висновку, що зберігання та пересилання даних за допомогою хмарних сховищ є більш швидким та надійним способом передачі інформації. Особливого прискорення активізації процесу застосування технологій хмарних обчислень у публічній та приватній сферах життя українського суспільства надало повномасштабне військове вторгнення на територію України, внаслідок якого під особливою загрозою кібератак опинилася інформація, що має стратегічне, критичне значення, та інформація, що має державну таємницю. Не зважаючи на велику кількість досліджень у сфері хмарних технологій, дану тему не можна вважати повністю вивченою. Особливо актуальним наразі є вивчення рівня захисту прав та інтересів учасників договірних відносин у сфері надання хмарних послуг за умови часткового обмеження конституційних прав та свобод громадян в період воєнного стану. Саме тому в роботі було проаналізовано ефективний зарубіжний досвід прийняття нормативно-правових актів, направлених на захист персональних даних користувачів хмарних послуг, правил ідентифікації користувачів даних послуг. У роботі наведено поняття хмарних технологій, еволюція їх розвитку у світі, а також законодавче визначення поняття персональних даних та їх конституційного захисту. У статті автором розглянуто сучасний рівень захисту прав та свобод учасників правовідносин з використання хмарних послуг у судах України. Також досліджено рівень застосування хмарних технологій державними органами, банківськими установами та підприємствами України під час війни, рівень дотримання ними прав та інтересів громадян під час використання таких технологій. Розглянуто законодавчо закріплені підстави для обробки персональних даних користувачів в період дії воєнного стану та норми про захист персональних даних користувачів хмарних послуг, які не діють під час особливого режиму в нашій державі. На підставі проведеного дослідження було дано оцінку сучасного рівня захисту прав та інтересів учасників правовідносин у сфері хмарних технологій.

Ключові слова: дата-центр, ідентифікація, технології хмарних обчислень, персональні дані, хмарний провайдер.

Yevlakhova E. R. **GENERAL THEORETICAL PRINCIPLES OF PROTECTION OF THE RIGHTS AND INTERESTS OF THE SUBJECTS OF CONTRACTUAL RELATIONS IN THE FIELD OF CLOUD COMPUTING TECHNOLOGIES**

Digitization of the global economy and all processes taking place in the world has long since begun to step forward at a very fast pace. Countries around the world have long come to the conclusion that storing and forwarding data using cloud storage is a faster and more reliable way to transfer information. A full-scale military invasion of the territory of Ukraine provided a special acceleration of the process of application of cloud computing technologies in the public and private spheres of Ukrainian society, as a result of which information of strategic and critical importance and information of state secret was under a special threat of cyber attacks. Despite the large amount of research in the field of cloud technologies, this topic cannot be considered fully studied. Studying the level of protection of the rights and interests of participants in contractual relations in the field of cloud service provision is particularly relevant at the moment, subject to partial restriction of the constitutional rights and freedoms of citizens during martial law. That is why the work analyzed the effective foreign experience of adopting legal acts aimed at protecting personal data of users of cloud services, rules for identifying users of data services. The work presents the concept of cloud technologies, the evolution of their development in the world, as well as the legislative definition of the concept of personal data and their constitutional protection. In the article, the author considered the current level of protection of the rights and freedoms of participants in legal relations for the use of cloud services in the courts of Ukraine. The level of application of cloud technologies by state bodies, banking institutions and enterprises of Ukraine during the war, the level of observance by them of the rights and interests of citizens during the use of such technologies was also investigated. The legally established grounds for the processing of personal data of users during the period of martial law and the rules on the protection of personal data of users of cloud services, which do not operate during the special regime in our country, are considered. Based on the conducted research, an assessment of the current level of protection of the rights and interests of participants in legal relations in the field of cloud technologies was given.

Key words: data center, identification, cloud computing technologies, personal data, cloud provider.

Вступ. Донедавна українське законодавство не мало спеціальних правових норм, якими було б враховано розвиток ІТ, що створювало проблему недостатньої правової визначеності. 17 лютого 2022 року в Україні прийнято Закон «Про хмарні послуги», який взяв за основу Директиви Європейського Союзу у сфері захисту персональних даних та електронних комунікаційних послуг. Саме даним законом нормативно врегульовано статус учасників правовідносин у сфері надання хмарних послуг, їх права та обов'язки, а також способи захисту їх прав у разі порушення.

Саме тому **метою** даного дослідження є аналіз загальнотеоретичних основ захисту прав та інтересів учасників договірних відносин у сфері застосування хмарних обчислень та надання оцінки сучасному рівню захисту цих прав.

У роботі буде досліджено поняття хмарних технологій, персональних даних та їх конституційний захист, в тому числі під час воєнного стану, а також зміни у діяльності органів державної влади, місцевого самоврядування, банківської системи та українських підприємств, обумовлені законодавчо закріпленим правом використання технологій хмарних обчислень, ефективна судова практика захисту прав та інтересів користувачів хмарних послуг.

Огляд літератури. В роботі буде проведено аналіз українських та зарубіжних публікацій, що досліджували проблеми захисту інформації у хмарних сховищах. Так у [26] американськими вченими П. Меллом та Т. Гренсом у їх роботі «Визначення хмарних обчислень NIST» найбільш повно визначено поняття хмарних обчислень, яке на сьогодні використовується у науковій літературі. У роботах українських вчених І.А. Близнюк та Н.А. Дмитрик [8; 9] розглянуто цифрову трансформацію сучасного суспільства, наведено найкращі моделі регулювання цифрових технологій. У роботі Т.А. Полякової та А.І. Хімченко, [18] проаналізовано європейський досвід прийняття Директив, направлених на регулювання сфери надання електронних комунікаційних послуг та захисту персональних даних під час їх реалізації.

Методологія дослідження складається з аналізу міжнародних документів та українського законодавства у сфері використання хмарних технологій, публікацій з проблеми дослідження, спостереження, порівняння, аналізу досвіду світового та вітчизняного застосування хмарних технологій.

Викладення основного матеріалу та обговорення результатів дослідження. Поняття «хмара» було використано вперше у 1977 році професором Рамнатхом Челлапа Університету Південної Каліфорнії як позначення обчислювального простору, що виникає між споживачем та провайдером. Саме цим професором та дослідником було сформовано сучасний погляд на явище хмарних технологій та визначено їх як обчислювальну парадигму, в якій межі обчислень визначаються не технічними можливостями, а економічним обґрунтуванням [12].

У 1999 році з'явився перший справжній хмарний сервіс Salesforce.com, яким було надано змогу користувачам використовувати власну CRM-систему через вказаний сайт на умовах передплати. Таким чином, Salesforce можна назвати першою компанією, якою було запропоновано SaaS-механізм для того, щоб розробити хмарні системи [12].

Вже у 2002 році подібна ідея була використана компанією Amazon, якою було створено хмарний сервіс під назвою AWS Platform, що став першим в історії справжнім хмарним сховищем. Компанія Amazon модернізувала власні центри обробки даних. Компанією було враховано, що більша частина комп'ютерних мереж протягом одного моменту часу використовує тільки 10% власної потужності, тому модернізація є вкрай необхідною для забезпечення надійності комп'ютерних мереж під час стрибків навантажень.

У 2009 році компаніями Google та Microsoft було запущено платформи у сфері хмарних технологій, якими можна ознаменувати завершення етапу становлення хмарних ресурсів та зроблено хмарні технології більш масовими для споживачів.

Найбільші на сьогодні хмарні провайдери створено компаніями Google, Microsoft та Amazon.

Аналітичною компанією IDC було підсумовано, що у 2009 році ринок хмарних послуг склав близько 17 млрд. дол. США, тобто 5% всього ринку інформаційних послуг, у 2016 році цей показник склав 83 млрд. дол. США. IDC зроблено прогноз зростання даного показника до 2023 року до 215 млрд. дол. США. Станом на сьогодні вже більше 50% компаній у всьому світі мають мінімум одне хмарне сховище для обміну внутрішньою інформацією між працівниками та обміну інформацією з контрагентами та клієнтами [11].

Наразі технології хмарних обчислень використовуються практично кожною компанією у роботі як в Україні, так і в інших країнах світу. Саме тому важливо розуміти, що являють собою хмарні обчислення, яка їх правова природа та засади захисту прав і свобод суб'єктів, що використовують технології хмарних обчислень на договірних засадах.

Найчастіше, хмарними обчисленнями називають модель роботи, з використанням якої підприємства отримують доступ до загального обчислювального ресурсу, що схожий на сервер, сховище, мережу або додаток, а також отримують доступ до інших хмарних послуг. Дані ресурси можуть бути використані та скеровані підприємством як користувачем без використання додаткових підказок та допомоги провайдера хмарної послуги.

Американськими вченими П. Меллом та Т. Гренсом у їх роботі «Визначення хмарних обчислень NIST» визначено хмарні обчислення моделлю для реалізації зручного мережевого доступу за потребою до спільного пулу, що має конфігуровані обчислювальні ресурси (мережі, сервери, сховища, програми та служби), що можуть бути швидко надані та вивільнені за докладання мінімальних зусиль під час керування та мінімальної взаємодії з постачальником таких послуг [26].

В ІТ-сфері поняття хмарного сховища та хмарних обчислень найчастіше замінюється терміном «хмара». Таким простим поняттям закривається складна система Інтернет-мережі, що має безліч технічних моментів.

Міжнародною організацією під назвою Інститут інженерів з електротехніки та електроніки у 2008 році було сформульовано власне визначення хмарних обчислень як своєрідної парадигми, в межах якої дані постійно зберігаються на сервері в Інтернеті і піддаються тимчасовому кешуванню на персональному комп'ютері, ігровій приставці, ноутбуці, смартфоні чи іншому гаджеті клієнта [25].

У Стратегії Європейської комісії під назвою «Розкриття потенціалу хмарних обчислень в Європі» поняття хмарних обчислень визначене як процес зберігання, обробки та застосування інформації на комп'ютерах, що розташовані дистанційно один від одного, шляхом застосування мережі Інтернет [21, с. 173].

Міжнародні правові акти мають свої визначення технологій хмарних обчислень. Так, Міжнародний союз електрозв'язку та Міжнародна організація по стандартизації (ICO) визначили хмарні комп'ютерні технології як парадигму забезпечення мережевого доступу до фізичних або електронних ресурсів, які піддаються масштабуванню, самостійному використанню та регулюванню клієнтами. Хмарними послугами вони називають послуги, надані або використані будь-якого зручного моменту клієнтами з використанням мережі Інтернет та будь-яких гаджетів, які використовують хмарні технології [24, с.17].

Закон України «Про хмарні послуги» визначає технологію хмарних обчислень як технологію, що забезпечує дистанційний доступ за потребою до хмарної інфраструктури, з використанням електронних комунікаційних мереж [4].

Таким чином, проаналізувавши всі наведені вище визначення, можна сформулювати визначення технологій хмарних обчислень як процесу надання доступу користувачам для зберігання та обчислення даних дистанційно, з використанням ресурсів провайдера.

Правовідносини у сфері технологій хмарних обчислень в Україні здійснюють на договірних засадах, що визначено Законом України «Про хмарні послуги», прийнятим 17 лютого 2022 року [4].

Саме договором про надання хмарних послуг наразі в нашій державі визначається порядок захисту даних користувачів хмарних послуг, зокрема їх персональних даних, від кібератак та інших несанкціонованих дій, внутрішньої та зовнішньої загрози, порядок оповіщення користувача хмарної послуги про інцидент, пов'язаний з кібербезпекою, що може вплинути на надання хмарної послуги, а також вимоги щодо безперебійності надання послуг хмарними провайдерами, вимоги щодо резервного копіювання даних користувачів, щодо порядку передачі даних від користувача до хмарного сховища, а також його доступу до цих даних та видалення їх з хмарного сховища у разі припинення договору. Договором також визначаються умови його припинення, а також відповідальність сторін договору (користувача хмарних послуг та надавача хмарних послуг) у разі порушення ними будь-якого пункту договору, зокрема порушення ними власних обов'язків та прав одне одного, передбачених договором.

Істотною умовою договору про надання хмарних послуг законодавством визначено також можливість захисту сторонами договору своїх прав та інтересів в судовому порядку у разі їх порушення. У випадку відсутності у договорі вказаного пункту про можливість судового оскарження такий договір може бути визнано недійсним в судовому порядку.

Таким чином, прийняття Закону України «Про хмарні послуги» можна вважати важливим кроком на шляху захисту прав та інтересів суб'єктів договірних відносин у сфері технологій хмарних обчислень, які активно розвиваються протягом останніх років. Кількість обчислювальних ресурсів, що використовуються в роботі державних органів, різко зростає з кожним роком, що породжує необхідність ефективного використання держбюджету та врегулювання процесу застосування хмарних технологій, а також зменшення навантаження на державні органи [14].

Відповідно до статистично-аналітичних даних економічного журналу «The Economist» об'єми цифрової інформації у всьому світі зростають кожні 5 років у 10 разів. Саме тому все більш ефективним стає принцип під назвою «Cloud First», тобто перенесення основних процесів виробництва у хмари. Реалізація даного принципу в Україні за прикладом розвинутих країн світу покликана зменшити корупційні ризики під час закупівель обладнання, зменшити витрати державного та місцевих бюджетів, наблизити інноваційний розвиток українських органів влади [14].

В Україні вже давно було визнано, що використання хмарних сервісів у державній політиці є успішним міжнародним досвідом, адже такі технології протягом багатьох років успішно діють в США, Сінгапурі, Німеччині, Індії, Австралії, Республіці Корея, Саудівській Аравії, Швеції, Данії, Норвегії, Великій Британії. Зокрема, в останній за допомогою хмар були зменшені витрати на цифрові трансформації та інформатизацію більш, ніж на 3 млрд. фунтів стерлінгів. У Данії муніципалітет, що відповідає за здійснення публічних закупівель, вже давно повністю перенесено на хмари, а в Норвегії – органам місцевого самоврядування

нині дозволено використовувати хмарні продукти у своїй діяльності. Успішний досвід використання хмарних технологій має і Швеція [14].

Отже, ще нещодавно вітчизняне законодавство не забезпечувало безпеку інформації при її віддаленій обробці у дата-центрах, а також захист прав та свобод суб'єктів, що використовують хмарні технології. Саме тому в основу діючого нині закону про хмарні послуги було покладено успішний міжнародний досвід та найкращі практики у даній сфері.

Головним чином, у США вже давно була розроблена процедура FedRAMP, яку мають проходити постачальники з метою одержання дозволу на надання хмарних послуг на федеральному рівні. Для щорічного продовження авторизації постачальники мають здійснювати відстеження власних засобів управління безпекою та проводити їх оцінку [20].

Інші економічно розвинені країни у всьому світі, починаючи з 2010 року, запровадили у своїй правовій сфері «Cloud First Strategy», редакцію якої було оновлено у 2018 році.

Європейським Союзом було прийнято програмні документи, що визначили пріоритетом Європейського Союзу розширення та поліпшення якості доступу до цифрових мереж, так звану «оцифрованість» світової економіки та економіки кожної окремої країни, а також стандартизацію у сфері хмарних технологій, 5G, Інтернету речей, інформаційних технологій та кібербезпеки:

– «Digital Agenda for Europe 2015» («Цифровий порядок денний для Європи 2015»);

– «Single Digital Market» («Єдиний цифровий ринок»);

– «In Industrial Policy for the Globalization Era» («Індустріальна політика ери глобалізації»);

– «The Innovation Union» («Інноваційний союз»).

Протягом останніх десятиліть хмарним обчисленням та правам учасників правовідносин, що з ними пов'язані, приділяється дуже пильна увага у Європейському Союзі. Зокрема у вересні 2012 року ЄС була прийнята стратегія, що отримала назву «Unleashing the Potential of Cloud Computing in Europe» («Розкриття потенціалу хмарних обчислень у Європі»). Даною стратегією ЄС стимулювало країн-учасниць до активного використання хмарних обчислень, аналізуючи власні політичні, нормативні та технологічні можливості. Трьома головними напрямками стратегії ЄС у сфері хмарних обчислень є [15]:

– безпечність та справедливість умов контракту, належний рівень захисту прав та інтересів учасників правовідносин у сфері використання технологій хмарних обчислень;

– спрощення більшості існуючих стандартів у сфері хмарних обчислень з метою підвищення їх доступності та прозорості для користувачів хмарних послуг;

– формування та реалізація так званого «європейського хмарного партнерства».

У грудні 2013 року Європарламентом було ухвалено Резолюцію про розкриття потенціалу хмарних сервісів та технологій, в якій було нормативно врегульовано та висвітлено важливі питання у сфері технологій хмарних обчислень [10]:

– можливість використання хмарних технологій для підвищення рівня зайнятості населення та економічного зростання;

– взаємодія європейського ринку та хмарних технологій;

– публічні закупівлі, а також закупівлі інноваційних рішень, у взаємодії з технологіями хмарних обчислень;

– хмарні обчислення та національні стандарти кожної окремої держави і ЄС в цілому;

– рівень захисту права інтелектуальної власності у технологіях хмарних обчислень та рівень дотримання діючого цивільного законодавства про відшкодування майнової та моральної шкоди за порушення законних прав і інтересів учасників правовідносин у сфері надання хмарних послуг;

– можливість дотримання належного рівня захисту персональних даних користувачів хмарних послуг та прав і інтересів звичайних громадян під час надання та використання хмарних послуг.

Внаслідок прийняття у 2013 році вищевказаної Резолюції Європарламенту, країнами учасницями ЄС було почергово прийнято спеціалізовані законодавчі акти про захист даних у сфері хмарних обчислень та захист прав і інтересів учасників таких правовідносин. Україною ж було прийнято спеціалізований закон у сфері надання хмарних послуг тільки у 2022 році.

Чехія однією з перших країн у 2013 році прийняла Закон про захист персональних даних у хмарних сервісах, який:

– визначив поняття хмарних обчислень;

– розмежував поняття Iaas, Paas, Saas, публічної хмари, приватної хмари і гібридної хмари;

– визначив поняття обробника та контролера даних;

– визначив правила щодо передачі персональних даних користувачів та правила передачі інформації через хмарні сховища за межі держави;

– визначив порядок оцінки адекватності рівня захисту;

– впровадив типовий договір про надання хмарних послуг, що передбачив істотні умови, зокрема права та обов'язки сторін, способи їх захисту у разі порушення та відповідальність сторін за порушення умов договору, а також прав та інтересів одне одного.

У Великій Британії ще у 1998 році було прийнято Закон про захист даних, а у 2012 році – Звід

керівних принципів у сфері хмарних обчислень для підприємств, в якому було розміщено вимоги до обробки даних у приватних, публічних та змішаних хмарах. У 2015 році в державі було прийнято Закон про цифрову економіку, що діяв до 2018 року.

Таким чином, можна прийти до висновку, що країни-члени Європейського Союзу ставлять високі вимоги до рівня захисту даних, розміщених на хмарних сховищах, зокрема до захисту персональних даних користувачів хмарних послуг. Необхідність обробки персональних даних користувачів таких послуг за допомогою хмарних обчислень створює деякі проблеми, що пов'язані із застосовним правом, визначенням регуляторів та провайдерів, а також умов договорів, які передбачають як самі хмарні послуги, так і міжнародну передачу даних.

Правила надання хмарних послуг у країнах, що належать до Європейської економічної зони, наразі регулюються Загальноєвропейським регламентом захисту даних (GDPR), що набув чинності у 2018 році [8].

Саме даним регламентом нормативно врегульовано обов'язковість захисту персональних даних та їх конфіденційності під час зберігання у хмарних сховищах та передачі за межі ЄС, а також уніфіковано регулювання та спрощено регуляторне середовище для міжнародного бізнесу.

Директиву №2009/136/ЄС про конфіденційність та електронні засоби зв'язку було прийнято у ЄС у 2013 році. У міжнародному правовому середовищі вона отримала назву Директива ePrivacy. Наразі в Європейському Союзі готується пакет змін, що мають бути внесені до даної директиви на підставі прийняття у 2018 році Загальноєвропейського регламенту захисту даних (GDPR) [8].

Директива ePrivacy покладена в основу нормативно-правової бази країн учасниць Європейського Союзу. Її важливість зводиться до того, що директивою [9]:

– врегульовано правила електронної комунікації, правила безпечної обробки даних та захисту приватного життя учасників відносин з використання хмарних обчислень;

– врегульовано правовідносини у сфері надання послуг електронного зв'язку;

– встановлено обов'язок надавачів послуг електронного зв'язку щодо забезпечення безпеки таких послуг;

– встановлено обов'язкову конфіденційність електронних повідомлень та даних щодо трафіку;

– визначено вимоги щодо конфіденційності кінцевого обладнання електронного зв'язку та обробки даних щодо трафіку;

– встановлено правила відправки повідомлень, що не запитуються.

Важливими для правового регулювання правовідносин у сфері хмарних обчислень є обидві Директиви Європейського Союзу, проте важливо пам'ятати, що головним регулюючим нормативно-правовим актом для кожної держави є її спеціальний закон про хмарні послуги, який має бути прийнятий та ратифікований у відповідності до норм міжнародного права та Директив ЄС зокрема [9].

Директивою ЄС про захист даних визначено поняття конфіденційних даних як особистих відомостей, якими розкривається етнічне та расове походження, філософські погляди, релігійні переконання, інформація щодо членства особи у різного роду спілках та угрупуваннях, а також інформація щодо статевого життя особи та стану її здоров'я. Директивою ЄС визначено, що до даних, які мають статус конфіденційних, застосовується спеціальний правовий режим, заснований на презумпції про те, що використання таких даних без згоди особи, якій вони належать, або неправильне використання таких даних може спричинити серйозні необоротні наслідки для прав та свобод людини.

Забезпечення безпеки персональних даних користувачів хмарних послуг європейське законодавство визначає ключовою умовою реалізації хмарних послуг. Саме тому визначено, що надавач хмарних послуг або послуг центру обробки даних зобов'язаний вживати усі технічні та організаційні заходи, що потрібні для захисту персональних даних користувачів хмарних послуг від кібератак, а також чужого незаконного посягання, від їх знищення, зміни чи спотворення. Даний обов'язок покладено в основу кожного спеціального закону у сфері хмарних послуг країн-учасниць ЄС, а також України, яка з 2022 року отримала статус кандидата на членство у Європейському Союзі, що говорить про те, що Україна максимально наблизила власне законодавство до європейського.

На сьогоднішній день у Європейському Союзі діє спеціальний міжнародний орган, компетенція якого поширюється на захист персональних даних користувачів хмарних послуг під час використання технологій хмарних обчислень, а саме: Європейське агентство мережевої та інформаційної безпеки (ENISA). Даним органом розробляються рекомендації та принципи відносно безпеки у хмарному середовищі та захисту від протиправних інцидентів, направлених на кібербезпеку.

Актуальними наразі є методи, що дозволяють пом'якшити ризики внаслідок обробки персональних даних під час використання технологій хмарних обчислень, Інтернету речей та великих баз даних. Ці ризики пов'язані з анонімним та псевдонімним відображенням даних та аутентифікацією учасників правовідносин у сфері використання технологій хмарних обчислень [18].

Отже, можна з впевненістю сказати, що саме Директивою Європейського Союзу про захист даних визначено головні засади захисту даних користувачів хмарних послуг, а отже захисту їх прав та інтересів. На основі цих засад має відбуватися обмін інформацією як з ідентифікованими, так і з не ідентифікованими особами, за обов'язкового вжиття надавачем хмарних послуг усіх можливих заходів для ідентифікації такої особи [16].

Вказана Директива ЄС містить поняття анонімізації користувача хмарних послуг у випадках необхідності збереження інформації на визначений термін та у формі, що допускає ідентифікацію [13].

На основі Директиви ЄС про захист даних країнами-членами ЄС було прийнято ряд нормативно-правових документів та підзаконних нормативних актів. Зокрема, у Франції було затверджено спеціальні посібники, що використовували затверджені Директивою ЄС положення щодо захисту даних. У Великобританії було затверджено практичні правила управління ризиками, що пов'язуються з анонімізацією користувачів хмарних послуг. Даним документом передбачено ризики анонімізації, що пов'язані з захистом персональних даних та ідентифікацією користувачів хмарних послуг, наведено приклади успішної анонімізації, наприклад, анонімізації медичних даних. У Великій Британії створено британську мережу анонімізації (UKAN), яка наразі допомагає країнам світу у обміні міжнародною практикою анонімізації в державному секторі [10].

Отже, можна стверджувати, що протягом останніх десятиліть хмарні технології активно розвиваються та отримують високу популярність саме завдяки своїй надійності, доступності та безпечності. Хмарні технології на сьогодні є важливими елементами цифрової економіки та цифрової екосистеми всього світу. Проте на сьогодні вже з'явилися технології, що можуть скласти серйозну конкуренцію хмарним обчисленням, а саме: технологічні платформи, що враховують розподілений реєстр (блокчейн-технології) IT-компаній Google та Apple.

Повномасштабне вторгнення Російської Федерації на територію України 24 лютого 2022 року дещо змінило правила ідентифікації та анонімізації користувачів хмарних послуг та перевірки даних, що розміщуються на хмарних платформах. До Закону України «Про хмарні послуги» внесено зміни, що стосуються заборони надавачам хмарних послуг розміщувати власну інфраструктуру на території країни-агресора або на території, тимчасово нею окупованій. Користувачам же хмарних послуг відтепер заборонено передавати до хмарних сховищ в межах України та за її межами інформацію, що може бути так чи інакше пов'язана з національною безпекою держави. Карається Кримінальним Кодексом України будь-яка допомога країні-агресору чи окупанту будь-якими засобами – розповсюдження матеріалів, листівок, ворожої символіки як у паперовому вигляді, так і в електронному, зокрема шляхом збереження їх на хмарному сховищі, та надання доступу до такої інформації іншим особам. З початку запровадження воєнного стану більш суворими стали правила ідентифікації користувачів хмарних послуг.

Саме тому особливо актуальним наразі стало питання захисту прав та інтересів користувачів хмарних послуг, гарантовані Конституцією України у статті 32, а саме [1]:

– заборонено втручання в особисте та сімейне життя осіб;

– заборонене збирання, використання та розповсюдження конфіденційних даних про осіб без наявності їх особистої згоди на це, за виключенням необхідності збереження національної безпеки, економічного благополуччя та захисту прав і свобод інших людей;

– громадяни України мають право ознайомлюватися в державних органах та органах місцевої вади з інформацією про себе, у випадку, якщо така інформація не складає державну таємницю;

– громадяни України мають право на судовий захист з метою спростування недостовірної інформації про себе, про членів своєї сім'ї, з метою вилучення такої інформації, відшкодування матеріальної та моральної шкоди, яка спричинена внаслідок збирання, зберігання та поширення недостовірних даних.

Саме з метою захисту особистих прав та інтересів громадян України, які на сьогодні в більшості своїй є користувачами хмарних послуг, був прийнятий Закон України «Про захист персональних даних». Відповідно до вказаного закону персональними даними є відомості або їх сукупність про певну фізичну особу, яка є ідентифікованою або може бути ідентифікованою. У відповідності до вказаного закону персональні дані можуть вважатися конфіденційною інформацією про особу, до якої за законом належать дані про національність людини, освіту, релігійні переконання, сімейний стан, стан здоров'я, адресу, дату народження та місце народження [2; 3].

У відповідності до діючого законодавства розпорядники персональних даних, в тому числі надавачі хмарних послуг, мають своїм обов'язком забезпечення захисту персональних даних від їх втрати чи знищення, несанкціонованої обробки або незаконного доступу.

Законодавством покладено контроль за захистом персональних даних громадян України, зокрема користувачів хмарних послуг, що використовують персональні дані, на Уповноваженого Верховної Ради України з прав людини та суди України.

Варто пам'ятати, що статтею 64 Конституції України передбачено можливість обмеження конституційних прав та свобод громадян України в період дії воєнного стану на території нашої держави. Таким чином, Указом Президента України №64/2022 від 24.02.2022 в Україні було введено воєнний стан та обмежено конституційні права і свободи людини та громадянина, зокрема встановлені статтею 32 Конституції.

Стаття 11 Закону України «Про захист персональних даних» визначає перелік підстав для обробки персональних даних будь-якої людини, зокрема і користувача хмарних послуг, а саме:

– згода суб'єкта персональних даних на таку обробку;

– дозвіл на обробку персональних даних, що наданий володільцю персональних даних, зокрема надавачу хмарних послуг, відповідно до закону для виконання його повноважень;

– укладення та виконання правочинів, стороною яких є суб'єкти персональних даних, або реалізація заходів, що передують укладенню правочину, за наявності згоди такого суб'єкта;

– захист життєво важливих прав та інтересів самого суб'єкта персональних даних;

– потреба у виконанні володільцем персональних даних свого обов'язку, передбаченого законом;

– потреба у захисті законного інтересу володільця персональних даних чи третьої особи, якій персональні дані передані, за виключенням випадків, коли потреба у захисті прав та свобод суб'єкта персональних даних важливіша.

Тобто наявність згоди самого суб'єкта персональних даних є тільки однією з шести підстав обробки його персональних даних. Тому навіть за відсутності згоди суб'єкта його персональні дані піддаються обробці за наявності інших п'яти підстав.

Закон «Про правовий режим воєнного стану» надав державним органам, військовому командуванню та адміністраціям, органам місцевого самоврядування повноваження, які необхідні для усунення загрози нашій державі, відсічі збройної агресії та досягнення належного рівня національної безпеки та незалежності України, її територіальної недоторканності та цілісності.

Таким чином, у період дії воєнного стану обов'язковими для обробки персональних даних суб'єктів є тільки дві підстави:

– дозвіл на обробку персональних даних, що наданий володільцю персональних даних, зокрема надавачу хмарних послуг, відповідно до закону для виконання його повноважень;

– потреба у виконанні володільцем персональних даних свого обов'язку, передбаченого законом.

Крім того, в період дії воєнного стану не застосовується стаття 7 Закону України «Про захист персональних даних» про заборону обробки даних щодо расового, етнічного походження особи, її політичних та релігійних переконань, світогляду, стану здоров'я, статевого життя, біометрики та генетики, у випадку, якщо обробка таких персональних даних необхідна для виконання вироків суду, виконання оперативно-розшукових завдань та завдань контррозвідки, боротьби з тероризмом, в межах повноважень, наданих законом органам державної влади та органам, що здійснюють оперативно-розшукову діяльність.

Отже, в період дії воєнного стану в нашій державі питання безпечності обробки персональних даних, їх захищеності від знищення, зміни чи обробки стало ще більш актуальним як для звичайних користувачів хмарних послуг, так і для державних органів та підприємств. Не зважаючи на призупинення дії деяких норм Конституції та спеціального законодавства України на період дії воєнного стану, обробка персональних даних має здійснюватися з урахуванням діючих положень законодавства України та дотримуючись принципів збереження національної безпеки, територіальної цілісності та недоторканності нашої держави.

Варто зазначити, що в українській судовій практиці є безліч рішень, винесених на користь звичайних громадян, що стали користувачами хмарних послуг або користувачами сторінок у соціальних мережах, направлених на захист їх прав та інтересів. Для прикладу можна навести постанову Броварського міськрайонного суду Київської області від 9 квітня 2020 року у справі №361/1579/20, що не була скасовано касаційною інстанцією. За матеріалами даної справи судом було встановлено, що в порушення вимог законодавства про захист персональних даних посадовими особами юридичної особи було розповсюджено персональні дані заявниці у месенджері Viber шляхом розміщення копії звернення заявниці до цієї юридичної особи, в якому були її прізвище, ім'я та по-батькові, номер мобільного телефону, адреса електронної пошти, адресі місця проживання. Внаслідок такого порушення персональні дані заявниці стали доступними для невизначеного кола осіб. Таким чином, посадовою особою юридичної особи було порушено ч. 3 ст. 10 та ч. 1 ст. 24 Закону «Про захист персональних даних» та вчинено адміністративне правопорушення, передбачене ч. 4 ст. 188-39 КУпАП.

Таким чином, можна стверджувати, що в Україні успішно функціонує інститут захист прав та інтересів суб'єктів персональних даних, зокрема і користувачів хмарних послуг, що надають свої персональні дані надавачам хмарних послуг для їх подальшої обробки.

8 березня 2022 року Національним банком України прийнято рішення про надання дозволу

банкам України використовувати у своїй діяльності хмарні послуги з метою розширення забезпечення стабільності функціонування української банківської системи в період воєнного стану. Тобто банками була отримана можливість надання банківських послуг, а також здійснення процесингу за операціями, використовуючи електронні платіжні засоби, в тому числі платіжні картки, хмарні сервіси, що реалізуються з використанням обладнання, яке фізично розміщене в державах ЄС, у США, Великій Британії та Канаді. Вказані зміни будуть продовжені ще протягом двох років після скасування воєнного стану [19].

Національний банк України також надав дозвіл банкам України в процесі проведення банківської операції та обробки персональних даних клієнтів, що відбуваються з використанням технологій хмарних обчислень, застосовувати українські засоби криптографічного захисту інформації, а також криптографічні засоби, що відповідають вимогам тієї держави, на території якої розміщується інфраструктура для надання хмарних послуг [5].

12 березня 2022 року Кабінетом Міністрів України було дозволено і державним органам використовувати хмарні сервіси, інфраструктура для надання яких знаходиться за межами території України у закордонних дата-центрах з метою убезпечення критично важливих даних під час дії воєнного стану на території України та з метою глобалізації цифрової трансформації нашої держави [22].

Прийняттю такого рішення передувала необхідність посилення безпеки нашої держави, адже важливі для України дані та інформація, що містить державну таємницю, протягом багатьох років зберігалися тільки на фізичних носіях інформації. До моменту перенесення таких даних у хмару, на фізичні носії інформації, що містять важливу для держави інформацію, почали масово полювати кіберзлочинці та російські ракети. Тобто використання технологій хмарних обчислень у роботі державних структур України покликано сприяти:

– збереженню даних від їх несанкціонованого знищення, втрати чи зміни;

– гарантованому резервному копіюванню даних державних органів;

– швидкому відновленню роботи державного органу чи апарату після фізичного пошкодження обладнання або спроби хакерської атаки;

– захисту даних, що містять державну таємницю та стратегічно важливу інформацію, від кібератак;

– стабільному доступу кожного громадянина до державних послуг навіть у період воєнного стану, що нерозривно пов'язано з захистом законних прав та інтересів громадян України;

– налаштуванню віддаленої роботи співробітників державних органів за відсутності можливості фізичної присутності на робочому місці за об'єктивними причинами.

На сьогодні можна впевнено сказати, що хмарним сервісом, якому найбільше довіряють українці та українські державні структури, є сервіс від компанії Microsoft – Microsoft Azure [22].

Отже, у банківській системі Україні та в роботі її державних органів сьогодні активно запрацювали технології хмарних обчислень з метою підвищення рівня безпеки усієї інформації, що передається на хмарні сховища, а також збереження та нерозповсюдження персональних даних громадян України. Можна з впевненістю стверджувати, що технології хмарних обчислень допомогли зробити рішучий крок назустріч підвищенню рівня захищеності прав та інтересі учасників договірних відносин у сфері технологій хмарних обчислень.

Висновки:

1. Прийняття Закону України «Про хмарні послуги» можна вважати важливим кроком на шляху захисту прав та інтересів суб'єктів договірних відносин у сфері технологій хмарних обчислень.

2. Європейським Союзом було прийнято програмні документи, що визначили пріоритетом Європейського Союзу розширення та поліпшення якості доступу до цифрових мереж, так звану «оцифрованість» світової економіки та економіки кожної окремої країни, а також стандартизацію у сфері хмарних технологій, 5G, Інтерету речей, інформаційних технологій та кібербезпеки. Забезпечення безпеки персональних даних користувачів хмарних послуг європейське законодавство визначає ключовою умовою реалізації хмарних послуг. Обов'язок захисту персональних даних користувачів хмарних сховищ, закріплений Директивами ЄС, покладено в основу Закону України «Про хмарні послуги».

3. У період дії воєнного стану обов'язковими для обробки персональних даних суб'єктів є тільки дві підстави з шести законодавчо закріплених: дозвіл на обробку персональних даних, що наданий володільцю персональних даних, зокрема надавачу хмарних послуг, відповідно до закону для виконання його повноважень; потреба у виконанні володільцем персональних даних свого обов'язку, передбаченого законом. Не діє в період воєнного стану і норма про захист персональних даних користувачів хмарних послуг, що пов'язані з їх політичними переконаннями, расовими особливостями, статевим життя, якщо такі дані необхідні для захисту національної безпеки України. Таким чином, в період дії воєнного стану в нашій державі захист прав користувачів хмарних послуг, що володіють персональними дани-

ми, є дещо обмеженим в інтересах захисту національної безпеки нашої держави.

4. У банківській системі Україні та в роботі її державних органів сьогодні активно запрацювали технології хмарних обчислень з метою підвищення рівня безпеки усієї інформації, що передається на хмарні сховища, а також збереження та нерозповсюдження персональних даних громадян України, що є беззаперечною гарантією їх захисту.

5. Можна стверджувати, що в Україні успішно функціонує інститут судового захисту прав та інтересів суб'єктів персональних даних, зокрема і користувачів хмарних послуг, що надають свої персональні дані надавачам хмарних послуг для їх подальшої обробки. Рівень захисту прав та інтересів учасників договірних відносин у сфері використання хмарних технологій в Україні можна назвати високим.

Література

1. Конституція України №254к/96-ВР від 28.06.1996 р. *Zakon.rada.gov.ua.* https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Про захист персональних даних: Закон України №2297-VI від 01 черв. 2010 р. *Zakon.rada.gov.ua. https://zakon.rada.gov.ua/laws/show/2297-17#Text*
3. Про інформацію: Закон України №2657-XII від 02.10.1992 р. *Zakon.rada.gov.ua. https://zakon.rada.gov.ua/laws/show/2657-12#Text*
4. Про хмарні послуги: Закон України №2075-IX від 17.02.2022 р. *Zakon.rada.gov.ua.* https://zakon.rada.gov.ua/laws/show/2075-20#Text
5. Про використання банками хмарних послуг в умовах воєнного стану в Україні: Постанова Правління Національного банку України №42 від 08.03.2022 р. *Bank.gov.ua.* https://bank.gov.ua/ua/legislation/Resolution_08032022_42
6. Абулов І.Ф., Горбенко І.Д. (2013). *Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі.* Прикладна радіоелектроніка.
7. Білова Т.Г., Ярута В.О. (2015). *Проблеми шифрування даних в хмарних обчисленнях.* Системи обробки інформації.
8. Близнюк І.А. (2018). *Цивільно-правова модель регулювання цифрових технологій.* КНУ.
9. Дмитрик Н.А. (2019). *Цифрова трансформація: правовий вимір.* Правознавство.
10. Дуккардт А.Н., Саєнко Д.С., Слєпцова Є.А. (2014). *Хмарні технології в освіті.* Відкрита освіта.
11. Історія (2020). *Sites.* https://sites.google.com/site/hmaarniobcislenna/home/istoria
12. Історія хмарних обчислень (2017). *Nachasi.* https://nachasi.com/tech/2017/09/26/istoriya-hmarnyh-obchyslen/
13. Касаткін П. А. (2016). *Хмарні обчислення - майбутнє світового ринку інформаційних технологій.* Науково-методичний електронний журнал Концепт.
14. Мінцифри: Законопроект про хмарні сервіси прийнято в цілому (2022). *KMU.GOV.UA.* https://www.kmu.gov.ua/news/mincifri-zakonoproekt-pro-hmarni-servisi-prijnyato-v-cilomu
15. Муравський В. В. (2018). *Комп'ютерно-комунікаційна форма обліку*. ТНЕУ.
16. Нікуліна О. В., Кізім А. А. (2014). *Хмарні технології як модель впровадження інновацій.* Наука та освіта: господарство та економіка; підприємництво; право та управління.
17. НКЦПФР запровадила нові умови використання хмарних сервісів на час війни (2022). *Юрліга.* https://jurliga.ligazakon.net/news/213056_nktspfr-zaprovadila-nov-umovi-vikoristannya-khmarnikh-servsv-na-chas-vyni
18. Полякова Т. А., Хімченко А. І. (2019). *Цифрова трансформація: правовий вимір.* Правознавство.
19. Про використання банками України хмарних послуг в умовах воєнного стану (2022). *Bank.gov.ua.* https://bank.gov.ua/ua/news/all/pro-vikoristannya-bankami-ukrayini-hmarnih-poslug-v-umovah-voyennogo-stanu
20. Рада схвалила закон про «хмару» для держорганів: чому це важливо (2022). *Epravda.* https://www.epravda.com.ua/news/2022/02/17/682468/ 9
21. Хатько А. (2016). *Можливості використання хмарних обчислень у системі інформаційного забезпечення хортингу.* Теорія і методика хортингу.
22. Хмари для держави: що можна використовувати під час війни (2022). *Kyivstar Business Hub.* https://hub.kyivstar.ua/news/hmary-dlya-derzhavy-shho-mozhna-vykorystovuvaty-pid-chas-vijny/
23. Чи реально притягти до відповідальності за порушення захисту персональних даних в Україні? (2021). *Всеукраїнське професійне юридичне видання: Юридична Газета online.* https://yur-gazeta.com/dumka-eksperta/chi-realno-prityagti-do-vidpovidalnosti-za-porushennya-zahistu-personalnih-danih-v-ukrayini.html
24. Чігіна Н.В. (2015). *Поняття та основні правові проблеми упорядкування відносин у сфері хмарних технологій*. Правова інформатика.
25. Hewitt C. (2008). ORGs for Scalable, Robust, Privacy-Friendly Client Cloud Computing. *Computer.* https://www.computer.org/csdl/magazine/ic/2008/05/mic2008050096/13rRUwhpBHv
26. Mell P., Grance T. (2011). The NIST Definition of Cloud Computing. *NIST.* https://csrc.nist.gov/publications/detail/sp/800-145/final