Принципи правового регулювання використання хмарних технологій для обробки персональних даних

Principles of Legal Regulation of the Use of Cloud Technologies for Personal Data Processing

Руслан Скриньковський [1], Ростислав Сопільник [1], Олександр Малашко [1]
Василь Віконський [1], Мирослав Ковалів [2], Тетяна Процюк [3], Сергій Єсімов [2], Роман Заяць [4]

Ruslan Skrynkovskyy, Rostyslav Sopilnyk, Oleksandr Malashko,
Vasyl Vikonskyi, Myroslav Kovaliv, Tetiana Protsiuk, Serhii Yesimov, Roman Zayats

[1] *Lviv University of Business and Law*
99 Kulparkivska Street, Lviv, 79021, Ukraine

[2] *Lviv State University of Internal Affairs*
26 Horodotska Street, Lviv, 79007, Ukraine

[3] *Academy of Financial Monitoring*
24 Biloruska Street, Kyiv, 04050, Ukraine

[4] *Lviv Scientific Research Forensic Center of the Ministry of Internal Affairs of Ukraine*
24 Koniushynna Street, Lviv, 79040, Ukraine

DOI: 10.22178/pos.60-9

JEL Classification: K40

Received 20.06.2020
Accepted 26.07.2020
Published online 31.07.2020

Corresponding Author:
Myroslav Kovaliv
mkovaliv1@ukr.net

Анотація. У статті досліджуються принципи правового регулювання, що формуються при використанні хмарних технологій для обробки персональних даних. Аналізуються нормативно-правові акти України, Європейського Союзу, самоврядних організацій, які об'єднують провайдерів хмарних інформаційних систем, що регулюють відносини у галузі персональних даних і використання хмарних технологій для обробки вказаних даних. Розглядаються окремі принципи правого регулювання використання хмарних технологій, зокрема: прозорості, законності, справедливості, мінімізації даних, «права на забуття» та портативності даних. Аналізуються правові засади діяльності операторів персональних даних і операторів систем хмарних технологій, досліджується вплив особливостей структури хмарних технологій на захист персональних даних. Також представлено пропозиції до проекту Закону України «Про хмарні обчислення».

Ключові слова: персональні дані; хмарні технології; обробка персональних даних; суб'єкти персональних даних; оператор хмарних технологій.

Abstract. The article studies the principles of legal regulation which are formed while using cloud technologies for personal data processing. The normative legal acts of Ukraine, of the European Union, self-governing organizations that unite providers of cloud information systems which regulate relations in the field of personal data and the use of cloud technologies for the processing of these data are analyzed. The article considers some principles of legal regulation of the use of cloud technologies, in particular: transparency, legality, fairness, data minimization, "the right to forget" and data portability. The legal bases of activity of operators of personal data and operators of systems of cloud technologies are analyzed, the influence of features of cloud technologies structure on protection of personal data is researched. Proposals to the draft of the "Cloud Computing" Law of Ukraine are also presented.

Keywords: personal data; cloud technologies; personal data processing; personal data subjects; cloud technology operator.

ВСТУП

Проблеми вибору ефективного механізму правового регулювання суспільних відносин, які складаються в процесі здійснення інформаційної діяльності з використанням хмарних технологій і персональних даних, стають актуальними в частині адаптації українського законодавства в інформаційній сфері до вимог Європейського Союзу. Розвиток інформаційно-комунікаційних технологій і зростаюча потреба в аналізі соціальних процесів на підставі персональних даних вимагають підвищення ефективності технологій обробки даних, що обумовлює необхідність удосконалення правового регулювання.

Проблемним питанням захисту персональних даних приділяється значна увага. Значний вклад у дослідження проблеми внесли вчені та практики: Г. Андрощук, О. Баранов, Ю. Батутін, В. Брижко, О. Кохановська, А. Новицький, В. Лопатін, Л. Сопільник, Р. Шишка та інші. Кожен з них зробив окремий внесок у вивчення й дослідження деяких питань, що стосуються політики безпеки персональних даних, але проблема правового регулювання відносин, що вникають при використанні хмарних обчислень для обробки персональних даних, потребує подальшого опрацювання.

Метою статті є дослідження принципів правового регулювання при використанні хмарних технологій для обробки персональних даних.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Науково-технічний прогрес зумовив широке впровадження інформаційних технологій в усіх галузях життєдіяльності суспільства. Роль інформаційних технологій полягає в підвищенні рівня ефективності виробництва, прибутку, конкурентоспроможності тощо не тільки за рахунок збільшення продуктивності праці, підвищення якості та швидкості прийняття управлінських рішень, але й за рахунок організації нових способів роботи з клієнтами і постачальниками. У даний час важливу роль стали відігравати хмарні технології. Все більше підприємств, установ та організацій розглядають можливість переходу до хмарних технологій, які мають великий потенціал для суттєвого підвищення ефективності без збитку для продуктивності. У процесі прийняття рішень про впровадження хмарних технологій щодо обробки інформації першорядним завданням є вибір кращих сервісів для впровадження, на основі аналізу правових і технічних факторів. Кожен з видів інформації схильний до ризику при обробці з використанням хмарних технологій.

У Європейському Союзі сформувалися принципи обробки даних з використанням хмарних інформаційних систем, які знайшли відображення у законодавстві України. Зокрема, в Законі України «Про інформацію» встановлені загальні принципи правового регулювання відносин у сфері інформації, в тому числі неприпустимість збору, зберігання, використання та поширення інформації про приватне життя особи без її згоди [1]. Поряд з тим, Закон України «Про захист персональних даних» деталізує принципи обробки персональних даних [2]. Дані принципи вимагають особливого підходу при розгляді та застосуванні в контексті використання хмарних технологій. Перший принцип обробки персональних даних з використанням хмарних технологій це прозорість. Як зазначає О. Баранов, динамічне та широке впровадження інформаційних технологій стало причиною появи достатньо великої множини суспільних відносин в різних сегментах суспільного життя, для яких окремі питання правового регулювання стало не зовсім очевидним, що створило окремі суттєві бар'єри на шляху їх застосування [3].

Схема надання доступу до хмарних технологій складна та закрита для перевірки. Невідомо, де знаходиться той комп'ютерний чіп, який обробив останній пошуковий запит. Відповідальність за вибір провайдера хмарних технологій несе саме фізична або юридична особа, яка прийняла рішення про використання хмарної інформаційної системи. Даний суб'єкт визначає кінцеву мету обробки даних та приймає рішення про можливість передачі даних для обробки та делегування всіх або частини прав і обов'язків зовнішній організації, яка фактично набуває статусу оператора персональних даних.

Провайдер хмарних технологій повинен надати можливість оцінки умов використання хмарної інформаційної системи. Суб'єкт персональних даних має бути забезпечений додатковою інформацією, особливо, якщо це необхідно для забезпечення дотримання йо-

го прав, в тому числі відомостями про факт і мету збору даних, про всіх залучених суб'єктів, про місця знаходження технічних засобів, що обробляють дані тощо. Повинна бути досягнута ясність в забезпеченні виконань зобов'язань суб'єктами, можливості залучення до відповідальності за невиконання або неналежне виконання обов'язків. Потенційні ризики можуть виникнути через необізнаність користувача про ланцюжок угод, який вибудовується при залученні співвиконавців провайдером хмарних технологій.

Прозорість повинна бути досягнута у всіх ланках ланцюжка в змісті відповідних угод: між суб'єктами персональних даних і операторами, операторами і особами, що обробляють дані.

Якщо надання корисних властивостей хмарних технологій вимагає установки програмного забезпечення замовником, провайдер хмарних технологій повинен інформувати про цю обставину, зокрема – про можливі наслідки з точки зору інформаційної безпеки та захисту даних.

З метою реалізації потенціалу хмарних технологій держави провайдери та користувачі повинні діяти таким чином, щоб подані правовідносини знаходилися у межах довіри та відповідно до чинного законодавства. Тут доцільно підтримати думку А. Новицького і О. Дяковського, які досліджуючи правове регулювання інформаційних баз даних, що містять персональні дані, зазначають, що Закон України «Про захист персональних даних» потребує внесення відповідних змін у частині правової охорони баз персональних даних шляхом запровадження обов'язкової реєстрації та формування Єдиного державного реєстру баз персональних даних [4].

Стратегія розвитку сфери інноваційної діяльності на період до 2030 року [5] передбачає створення правого механізму забезпечення довіри щодо використання інформаційно-комунікаційних технологій, але сьогодні зазначена проблема не вирішена.

У зв'язку з розвитком і вразливістю хмарних інформаційних систем провайдерам з кожним роком доводиться докладати все більше зусиль, щоб сформувати таку довіру користувачів у галузі конфіденційності та безпеки даних, інакше вони зіткнуться зі спадом попиту на пропоновані послуги.

Звідси очевидно, що в контексті використання хмарних технологій під прозорістю слід розуміти забезпечення достатності інформації про процеси, що відбуваються при функціонуванні хмарної інформаційної системи.

Дотримання принципів законності та справедливості щодо обробки даних при використанні властивостей хмарних технологій залежить від дотримання загальних та спеціальних принципів захисту даних. Джерело отримання даних є одним з критеріїв оцінки законності та справедливості обробки даних.

Так, Закон України «Про захист персональних даних» [2] в якості основної умови обробки персональних даних встановлює згоду суб'єкта персональних даних на обробку персональних даних. Це означає, що суб'єкти даних повинні чітко розуміти, що відбуватиметься з їх даними. Якщо персональні дані зібрані для однієї мети, а потім, у рамках аналітики великих даних були використані для інших цілей, суб'єкти персональних даних повинні бути завчасно сповіщені. Це особливо важливо, якщо організація планує використовувати дані з невідомою для особи метою. Ключовий фактор при визначенні нової мети сумісної з первісною полягає в мотивації особи, що приймає рішення про обробку персональних даних. Має значення оцінка, наскільки нова мета обробки даних зачіпає недоторканність приватного життя конкретних людей і чи відповідає вона очікуванням щодо використання особистої інформації.

У зазначеному аспекті О. Гронь і А. Погореленко у науковій праці [6] відображають проблеми у використанні хмарних технологій, зазначаючи, що правники характеризують Закон України «Про захист персональних даних» як не досить досконалий у зв'язку з відсутністю диференціації персональних даних на вразливі та звичайні, як це має місце у міжнародних документах.

Справедливість має на увазі розширену оцінку того, наскільки обробка інформації відповідає виправданим очікуванням конкретних людей. Існує різниця між використанням персональних даних, коли мета обробки збігається з причиною звернення людей до якогось сервісу, та коли дані використовуються з метою, відмінною від наданої послуги. Приклад першого це торгова компанія, яка використовує дані карт постійного покупця для ринкового дослідження. Приклад другого –

соціальна мережа, що надає дані для ринкового дослідження. Це не означає, що друге обов'язково нечесно.

Дотримання принципу законності та справедливості обробки даних залежить від змісту угоди про обробку персональних даних, схваленого користувачем при реєстрації та використанні послуг соціальної мережі, що функціонує з використанням хмарних технологій. Важливо, щоб користувачі були повідомлені, що станеться з їх даними, якщо вони приймуть рішення скористатися послугою.

Користувачі не повинні позбавлятися можливості використовувати хмарне програмне забезпечення в Інтернеті тільки тому, що вони не дали згоду на доступ до персональних даних для комерційного використання.

Посилення контролю за обробкою персональних даних здійснюється з акцентом на посилення принципу мінімізації використовуваних відомостей, регламентацією зберігання персональних даних, яка відповідно до Закону України «Про захист персональних даних» [2] має здійснюватися у формі, що дозволяє визначити суб'єкта персональних даних не довше, ніж цього вимагає мета обробки персональних даних. Оброблювані персональні дані підлягають знищенню або знеособленню після досягнення цілей обробки або в разі втрати необхідності в досягненні цих цілей.

Законодавство України як закони про захист даних держав Європейського Союзу, слідуючи міжнародним тенденціям, втілює концепцію мінімізації даних. Організації повинні мінімізувати обсяг зібраних і збережених даних, включаючи термін їх зберігання [7].

Вимога про термін зберігання даних не довше необхідного для мети збору підтримує принцип недоторканності приватного життя та відображає порядність в управлінні персональними даними. Однак, у межах особливостей концепції хмарних технологій, це може стати потенційними труднощами у зв'язку з прямими та непрямими чинниками. Збільшення обсягів даних і падіння вартості зберігання, саме за рахунок хмарних технологій, та здатність аналітики великих даних обробляти дуже великі обсяги даних може спонукати операторів до тривалого зберігання історичних архівів, що виходять за терміни і які необхідні для звичайної підприємницької мети. Україна в підтримці хмарного сервісу *CAEaaS* (англ. *Computer Aided Engineering as a Service*, комп'ютерні системи інженерного аналізу як сервіс) робить лише перші кроки, а забезпечити технологічні потреби підприємств, установ і організацій сьогодні може виключно при умові залучення закордонних постачальників. Якщо мова йде про економічну доцільність використання українських центрів обробки даних, то тут перевага – за меншою віддаленістю постачальника [8].

Організація можливості суб'єкта персональних даних управляти персональними даними повинна бути умовою використання хмарних технологій. Закон України «Про захист персональних даних» [2] надає суб'єктам даних права доступу до персональних даних, що знаходяться в обробці. Ці права продовжують діяти при використанні хмарних технологій.

Забезпечення доступності означає забезпечення можливості своєчасного та надійного доступу до особистих даних, в тому числі – доступу, виправлення, видалення або блокування інформації про приватне життя. У суб'єктів персональних даних залишається право отримувати копію інформації, що містить персональні дані, інформацію про джерела цих даних тощо.

Існування права зобов'язує операторів та осіб, які здійснюють обробку до роботи з даними у межах нормативного регулювання. Їм потрібно мати адекватні метадані (реквізити), можливість уточнення архівів, щоб знаходити всю наявну інформацію про суб'єкта персональних даних, знати про те, чи були дані, оброблені ними, дійсно анонімні або як їх можна пов'язати з конкретними особами. Якщо можливо надавати персональні дані таким способом, це допоможе операторам виконувати обов'язки із захисту даних, надати інформацію суб'єкту даних про те, який є обсяг і вид інформації.

Принцип портативності даних, який передбачений засадами реалізації органами виконавчої влади принципів державної політики цифрового розвитку, відповідно до [9] повинен забезпечувати можливість перенесення інформації особистого характеру на вимогу відповідної особи наскільки це технічно можливо, швидко та безперешкодно.

Ряд провайдерів хмарних технологій поки не використовують стандартні формати даних і послуг, інтерфейси сприяння сумісності та

перенесення даних між різними інформаційними системами. Якщо замовник вирішує змінити провайдера хмарних технологій, то це може стати практично неможливо або складно у зв'язку з труднощами передачі даних.

Особлива увага в аспекті гарантії прав користувачів повинна бути приділена «праву бути забутим» (англ. *Right to be forgotten*). Право на забуття включає забезпечення провайдерами та всіма суб'єктами виконавця можливості видалення персональних даних у повному обсязі після закінчення необхідності використання в легальних цілях, після відкликання згоди на обробку або після закінчення терміну дозволеного зберігання інформації.

Даний принцип отримав визначення у судових рішеннях Європейського суду з прав людини. Видалення даних, відповідне принципам безпеки, вимагає, щоб носії даних були повністю знищені або розмагнічені.

Специфічні технічні характеристики хмарних технологій дозволяють містити персональні дані одночасно в декількох копіях в територіально віддалених центрах обробки даних. Необхідно забезпечити і упевнитися, що кожен екземпляр даних був стертий безповоротно. У разі якщо повне знищення окремих даних неможливо відповідно до закону (наприклад, податкового законодавства), доступ до цих даних повинен бути заблокований.

Питання якості даних повинне бути враховане провайдером хмарних технологій, в тому числі щодо цілісності даних, автентичності та відносної незалежності від навмисних або випадкових змін в процесі обробки, зберігання або передачі. Поняття цілісності може бути поширене на хмарні інформаційні системи, що вимагає при обробці персональних даних інформацію залишити незмінною.

Держави Європейського Союзу сьогодні вживають всі необхідні заходи щодо досягнення високого якісного рівня надання послуг хмарних технологій з точки зору роботи з інформацією, що підпадає під поняття персональних даних. Серед підходів, яких дотримуються країни-члени Європейського Союзу при загальному регулюванні використання персональних даних, зустрічаються крайні підходи: від максимального захисту таких даних до майже повного заперечення права на анонімність в мережевих комунікаціях.

У науці неодноразово піднімалося питання розриву між практикою організації мережевих інформаційних систем і відповідності цієї практики реалізованим підходам правового регулювання інформаційних правовідносин. При наявності певного масиву регулятивних документів відзначається недостатність для вирішення об'єктивних проблем.

Сьогодні, коли кількість користувачів хмарних інформаційних систем і мережі Інтернет зростає високими темпами, багатьом традиційним інститутам і ієрархічним структурам доведеться змінитися, або вони істотно застаріють, переставши відповідати вимогам суспільства.

Стратегія «Вивільнення потенціалу хмарних обчислень в Європі» (англ. *Unleashing the potential of cloud computing in Europe*) передбачає впровадження схем сертифікації (галузевий групою по хмарних обчислень (*C-SIG*), підгрупою з розробки схем сертифікації (*SIG-Cert*) за участю Агентства з мережевої і інформаційної безпеки (*ENISA*) [10]. Надання допомоги у виборі безпечної та надійної хмарної інформаційної системи користувачам з приватного та публічного секторів стало основною метою впровадження схем сертифікації, оскільки використання хмарних технологій здійснюється на основі моделі з різними технологічними компонентами.

З огляду на те, що потік призначених для користувача даних великий, в разі здійснення оцінки виконання хмарним провайдером вимог до безпеки кожним клієнтом, робота буде дублюватися. Концепція сертифікації – одноразова кваліфікована перевірка базового набору вимог до безпеки, що оптимізує процедуру користувальницького вибору. Схеми сертифікації не замінюють необхідність належної «хмари» при виборі хмарного провайдера, а тільки спрощують цей процес. Попередньою умовою використання хмарної інформаційної системи для обробки персональних даних повинна бути комплексна, повна та кваліфікована оцінка технічних, організаційних і правових аспектів її функціонування.

Багато суб'єктів, що надають послуги з використанням мережі Інтернет усвідомили відповідальність та можливі наслідки користування сучасними технологіями. З огляду на те, що зростає кількість хмарних інформаційних систем і хмарних провайдерів, вибір для користувача є складний, але важливий. У даний час надається значення сформованому

іміджу компанії з позиції інформаційної безпеки, оскільки розібратися в складних правових моментах не просто. Даний факт є передумовою для розвитку інституту незалежної оцінки діяльності хмарних провайдерів, що вже отримала свій розвиток в державах-членах Європейського Союзу.

Інструмент попередньої оцінки та посвідчення рівня безпеки покликаний полегшити для користувача вибір і сприяти розвитку правовідносин щодо використання хмарних технологій в безпечному правовому полі. Концепція сертифікації відповідно до Стратегії «Вивільнення потенціалу хмарних обчислень в Європі» [10] реалізується самоврядними організаціями. Правила з організації надання корисних властивостей хмарних технологій, що належать до категорії саморегулювання, на добровільних засадах дотримуються усіма членами організації. Саме на даному рівні є доцільним формулювати правила для проведення оцінки діяльності провайдера хмарних технологій і самих хмарних інформаційних систем, та безпосередньо організовувати діяльність з аудиту хмарних технологій. Особливості структури інститутів громадського саморегулювання обумовлюють можливість реалізації такої оцінки на локальному, регіональному, національному рівнях та рівні ЄС.

Особливої уваги потребує принцип «забезпечення уніфікованого захисту персональних даних», тобто надання єдиного рівня захисту прав громадян незалежно національності оператора таких даних і того, в якій точці світу персональні дані обробляються, де географічно розташовані обчислювальні технології як елемент хмарної інформаційної системи, провайдер [11]. Реалізація даного принципу є досить складним завданням з погляду на транскордонну передачу оброблюваної інформації як специфіку використання хмарних технологій. У межах Європейського Союзу зазначене питання на технологічному рівні вирішено.

Якісною відмінністю хмарних інформаційних систем від традиційних є географічна віддаленість обчислювальних ресурсів від користувача, дублювання оброблюваної інформації і одночасне зберігання копій в декількох центрах обробки даних. Даний факт ускладнює дотримання принципу уніфікованого рівня захисту персональних даних, закріпленого національним правом користувача в Україні.

Обов'язки щодо захисту конфіденційних даних та охорони таємниці приватного життя лежать на всіх: на користувачах як суб'єктів персональних даних, на бізнесі, на громадських інститутах. Держави роблять спроби регулювати правовідносини, що виникають, великі провайдери, піклуючись про репутацію, оберігають дані, захищають інформаційні системи від злому та забезпечують користувачів ефективними засобами для максимального контролю в забезпеченні особистої безпеки. Застосування цих засобів залежить від користувачів.

Правове регулювання відносин з використання хмарних технологій повинно враховувати комплексний характер предмета регулювання при використанні хмарних технологій, що передбачає перехід від детального регулювання прав і обов'язків учасників відносин до регулювання принципів і технологічну нейтральність законодавства, що визначає максимальну незалежність регулювання від технологій, норми повинні застосовуватися учасниками відносин незалежно від зміни технологій. Регуляторні функції доцільно передати недержавним інституціям, що об'єднують учасників відповідних відносин. Це доцільно відобразити у проекті Закону України «Про хмарні послуги» [12].

В аналітичній записці Національного інституту стратегічних досліджень при Президентові України [13] жодна із зазначених вище проблем не піднімалась. Це не говорить про те, що ці проблеми не існували. Актуалізація проблем, у першу чергу, зумовлена чинниками інформаційної безпеки, які докладно визначені у Законі України «Про національну безпеку України» [14].

ВИСНОВКИ

Проблема забезпечення конфіденційності персональних даних при використанні хмарних технологій зачіпає користувача як суб'єкта або оператора персональних даних відповідального за вибір хмарної інформаційної системи та дотримання порядку безпечного використання. Вибір оператора хмарних технологій заснований на оцінці діяльності провайдера хмарних технологій у галузі інформаційної безпеки, охоплює аналіз мети і умов обробки персональних даних при згоді на обробку та дотриманні запобіжних заходів

при користуванні хмарною інформаційною системою. Провайдер хмарних технологій несе юридичну відповідальність за забезпечення конфіденційності персональних даних у межах Закону України «Про захист персональних даних» з урахуванням специфіки функціонування хмарних інформаційних систем. Телекомунікаційний оператор зв'язку відповідає за забезпечення конфіденційності персональних даних при організації мережевого доступу до хмарної інформаційній системі відповідно до законодавства про захист персональних даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

1. Pro informatsiiu [About information] (Ukraine), 02.10.1992, No 2657- XII. Retrieved July 1, 2020, from https://zakon.rada.gov.ua/laws/show/2657-12#Text (in Ukrainian)
   [Про інформацію (Україна), 02.10.1992, № 2657-XII. Актуально на 01.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text].
2. Pro zakhyst personalnykh danykh [About personal data protection] (Ukraine), 01.06.2010, No 2297-VI. Retrieved July 1, 2020, from https://zakon.rada.gov.ua/laws/show/2297-17#Text (in Ukrainian)
   [Про захист персональних даних (Україна), 01.06.2010, № 2297-VI. Актуально на 01.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text].
3. Baranov, O. A. (2016). Napriamy perspektyvnykh doslidzhen u haluzi informatsiinoho prava [Areas of prospective research in the field of information law]. *Informatsiia i pravo, 2*(17), 15–31 (in Ukrainian)
   [Баранов, О. А. (2016). Напрями перспективних досліджень у галузі інформаційного права. *Інформація і право, 2*(17), 15–31].
4. Novytskyi, A., & Diakovskyi, O. (2017). Pravove rehuliuvannia informatsiinykh baz danykh, shcho mistiat personalni dani [Legal regulation of information databases containing personal data]. *Pidpryiemnytstvo, hospodarstvo i pravo, 10*, 177–181 (in Ukrainian)
   [Новицький, А., & Дяковський, О. (2017). Правове регулювання інформаційних баз даних, що містять персональні дані. *Підприємництво, господарство і право, 10*, 177–181].
5. Pro skhvalennia Stratehii rozvytku sfery innovatsiinoi diialnosti na period do 2030 roku [On approval of the Strategy for the development of innovation for the period up to 2030] (Ukraine), 10.07.2019, No 526-p. Retrieved July 1, 2020, from https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80#Text (in UKrainian)
   [Про схвалення Стратегії розвитку сфери інноваційної діяльності на період до 2030 року (Україна), 10.07.2019, № 526-р. Актуально на 01.07.2020. URL: https://zakon.rada.gov.ua/laws/show/526-2019-%D1%80#Text].
6. Hron, O. V., & Pohorelenko, A. K. (2018). Problemy zakhystu personalnykh danykh u konteksti suchasnoi komunikatsii [Personal data protection problems within the context of modern communications]. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo, 19*(1), 102–108 (in Ukrainian)
   [Гронь, О. В., & Погореленко, А. К. (2018). Проблеми захисту персональних даних у контексті сучасної комунікації. *Науковий вісник Ужгородського національного університету. Серія: Міжнародні економічні відносини та світове господарство, 19*(1), 102–108].
7. Pro zatverdzhennia dokumentiv u sferi zakhystu personalnykh danykh [On approval of documents in the field of personal data protection] (Ukraine), 08.01.2014, No 1/02-14. Retrieved July 1, 2020, from https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text (in Ukrainian)
   [Про затвердження документів у сфері захисту персональних даних (Україна), 08.01.2014, № 1/02-14. Актуально на 01.07.2020. URL: https://zakon.rada.gov.ua/laws/show/v1_02715-14#Text].

8. Smirnova, T., Polishchuk, L., Smirnov, O., Buravchenko, K., & Makevnin, A. (2020). Research of cloudy technologies as a services. *Cybersecurity: Education, Science, Technique, 3*(7), 43–62. doi: 10.28925/2663-4023.2020.7.4362

9. Deiaki pytannia tsyfrovoho rozvytku [Some issues of digital development] (Ukraine), 30.01.2019, No 56. Retrieved July 1, 2020, from https://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF#Text (in Ukrainian)
[Деякі питання цифрового розвитку (Україна), 30.01.2019, № 56. Актуально на 01.07.2020. URL: https://zakon.rada.gov.ua/laws/show/56-2019-%D0%BF#Text].

10. European Commission. (2012). *Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions*. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

11. European Union Agency for Fundamental Rights and Council of Europe. (2014). *Handbook on European data protection law*. Retrieved from https://rm.coe.int/16805966a8 (in Ukrainian)
[Агенція Європейського Союзу з питань основоположних прав та Рада Європи. (2014). *Посібник з європейського права у сфері захисту персональних даних*. URL: https://rm.coe.int/16805966a8].

12. Pro khmarni posluhy [About cloud services] (Ukraine), 20.12.2019, No 2655. Retrieved July 1, 2020, from http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67744 (in Ukrainian)
[Про хмарні послуги (Україна), 20.12.2019, № 2655. Актуально на 01.07.2020. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67744].

13. Hnatiuk, S. L. (2013, March 5). *Aktualni pytannia zakhystu personalnykh danykh u virtualnomu seredovyshchi (na prykladi tekhnolohii ta servisiv "khmarnoho" obchyslennia)* [Current issues of personal data protection in the virtual environment (on the example of technologies and services of "cloud" computing)]. Retrieved from https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/aktualni-pitannya-zakhistu-personalnikh-danikh-u-virtualnomu (in Ukrainian)
[Гнатюк, С. Л. (2013, Березень 5). *Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів «хмарного» обчислення)*. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/aktualni-pitannya-zakhistu-personalnikh-danikh-u-virtualnomu].

14. Pro natsionalnu bezpeku Ukrainy [On the national security of Ukraine] (Ukraine), 21.06.2018, No 2469-VIII. Retrieved July 1, 2020, from https://zakon.rada.gov.ua/laws/show/2469-19#Text (in Ukrainian)
[Про національну безпеку України (Україна), 21.06.2018, № 2469-VIII. Актуально на 01.07.2020. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text].