ВОЛОХ О. К.,
кандидат юридичних наук,
доцент кафедри
адміністративного права і процесу
*(Національна академія
внутрішніх справ)*

УДК 35.077.2

ОБРОБКА ІНФОРМАЦІЇ В СИСТЕМАХ ХМАРНИХ ОБЧИСЛЕНЬ

У статті розглядаються питання щодо доцільності застосування у діяльності публічної адміністрації «хмарних» технологій. Обґрунтовуються ризики для інтересів національної безпеки внаслідок обробки інформації в системах хмарних обчислень. Висвітлюються питання захисту об'єктів критичної інформаційної інфраструктури держави.

Ключові слова: *хмарні обчислення, національна безпека, обробка інформації, критична інформаційна інфраструктура, персональні дані.*

В статье рассматриваются вопросы целесообразности применения в деятельности публичной администрации «облачных» технологий. Обосновываются риски для интересов национальной безопасности вследствие обработки информации в системах облачных вычислений. Освещаются вопросы защиты объектов критической информационной инфраструктуры государства.

Ключевые слова: *облачные вычисления, национальная безопасность, обработка информации, критическая информационная инфраструктура, персональные данные.*

The article deals with the question of whether the use of public administration in the "cloud technologies. Substantiated risks to national security because of information processing systems in cloud computing. The issue of protecting critical information infrastructure of the state.

Key words: *cloud computing, national security, information processing, critical information infrastructure, personal data.*

Вступ. На розгляд парламенту подано проект Закону України «Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень» (реєстр. від 24 березня 2016 р. № 4302).

Слід вказати, що тема так званих хмарних технологій (сервісів, обчислень) вже не перший рік обговорюється в суспільстві. Відповідно, є певні напрацювання і в нормативно-правовій, і в науково-технічній сферах.

Ще в 2013 р. у Стратегії розвитку інформаційного суспільства було сформульовано, що одним з основних напрямів реалізації Стратегії є розвиток такої сфери суспільного життя, як інформаційна інфраструктура. Формування сучасної інформаційної інфраструктури, як зазначається далі, передбачає створення та застосування суперкомп'ютерних систем, зокрема на основі «хмарних» технологій [1]. Як вказується нижче, практично доведені ризики для безпеки інформації в результаті її обробки в системах хмарних обчислень. Однак керівництво нашої держави з певних причин не вважає їх значними, хоча озвучені вони були у доповідях фахівців Національного інституту стратегічних досліджень (далі – НІСД).

Постановка завдання. Метою статті є дослідження питання доцільності застосування у діяльності публічної адміністрації «хмарних» технологій у зв'язку з розвитком електронного урядування в Україні.

Результати дослідження. Хмарні обчислення (англ. *cloud computing*) – модель забезпечення повсюдного і стабільного мережевого доступу на вимогу до комплексу програмних та апаратних обчислювальних ресурсів (наприклад, до серверів, сховищ даних, програмного забезпечення, сервісів, інфраструктурних мереж – як у конфігурації, так і окремо), які можуть бути оперативно надані й відкликані з мінімальними експлуатаційними витратами та/або зверненнями до провайдера [2].

У свідомість громадян цілеспрямовано впроваджується думка про те, що хмарні обчислювання сьогодні є актуальним підходом до створення пов'язаних з інформаційними технологіями продуктів та рішень, який найближчим часом охопить всі галузі обробки інформації: «Хмарні обчислення допоможуть зберігати надвеликі обсяги даних з доступом з мобільних та персональних комп'ютерів. Такі сервіси вже доступні з мінімальними фінансовими витратами або навіть надаються безкоштовно» [3].

На офіційному сайті компанії Microsoft-Україна є рекламна інформація такого змісту: «Спробуйте безкоштовно хмарні технології Microsoft – працюйте ефективніше у захищеному мобільному середовищі. Спробуйте безкоштовно наші сервіси зараз та придбайте їх із чудовою знижкою» [4].

Аналіз наявних джерел свідчить про те, що суб'єктами лобіювання впровадження хмарних технологій та прийняття з цією метою відповідного законодавства наполегливо акцентується на економії коштів (приватних або державних), перспективності хмарних технологій, простоті і, нарешті, на безальтернативності їх використання, зокрема в діяльності органів публічної адміністрації.

Однак будь-який потенційний споживач хмарних технологій (і народні депутати України в тому числі) повинен завжди пам'ятати відоме правило: якщо пропонують щось задешево або безкоштовно, обов'язково існує не декларована, а дійсна мета такої пропозиції.

У нашому розпорядженні є дві аналітичні записки експертів НІСД з питань впровадження хмарних технологій і наявного досвіду західних держав у цьому напрямі.

В аналітичній записці під назвою «Перспективи розвитку хмарних обчислень в Україні: переваги та ризики» розглядаються переважно позитивні сторони запровадження хмарних технологій в Україні. Зокрема, надано такі *висновки та рекомендації.*

1) Сучасні хмарні технології (cloud computing) є прогресивним та перспективним рішенням, одним з елементів революційної «третьої IT-платформи». Їх швидке поширення зараз є одним з тих ключових трендів, що в найближчі 5–8 років помітно вплинуть на глобальний розвиток. У найрозвиненіших регіонах світу (США, ЄС) вже прийняті стратегічні рішення та плани дій щодо системного та комплексного розвитку хмарних сервісів, розгорнута відповідна робота.

2) Використання хмарних технологій пов'язане не лише з величезним зменшенням витрат та інтенсифікацією, але і зі значущими споживацькими ризиками (передусім з ризиками зберігання та передачі даних). З іншого боку, хмарні рішення весь час вдосконалюються, а крім того, хмарний провайдер сьогодні може досягти прийнятного рівня безпеки, дотримуючись низки умов [5].

Щодо «значущих споживацьких ризиків» більш детальна інформація міститься в аналітичній записці, яка має назву «Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів «хмарного»" обчислення)» [4]. У ній йдеться про те, що, незважаючи на стрімкий розвиток «хмарних» сервісів, їм притаманні і високі ризики використання. Справа у тому, що завдяки особливостям свого функціонування «хмарні» сервіси створюють цілком специфічне середовище, в якому традиційні нормативно-правові механізми, практики та підходи є здебільшого неефективними.

У квітні 2012 р. авторитетна міжнародна команда експертів з захисту персональних даних у телекомунікаційних мережах («Берлінська група») опублікувала результати спеці-

ального профільного дослідження, що отримало назву «Сопотський меморандум». У документі фіксуються, зокрема, такі проблеми та ризики використання «хмар»:

– дотримання конфіденційності, недоторканості інформації та режиму доступу до неї не може бути проконтрольоване у «хмарах»;

– під час передачі персональні дані потрапляють під юрисдикції, в яких не передбачено їх адекватного захисту;

– провайдери та їх партнери використовують приватні дані у своїх інтересах без повідомлення про це володільця та його згоди;

– локальні (національні) контролюючі інститути з захисту персональних даних фактично не мають можливості нагляду за процесом обробки даних провайдерами «хмарних» послуг [6].

Зазначені висновки експертів цілком підтверджуються наявними цифрами та фактами. Зокрема, результати глобального дослідження "Avoiding the Hidden Costs of the Cloud" вказують на значний відсоток недоброчесних гравців на ринку «хмарних» послуг. Так, 77% респондентів щонайменше один раз стикалися з шахрайськими сервісами, а 40% з них стали жертвами викрадення конфіденційних даних [7].

Додатковим підтвердженням недостатньої надійності сучасних «хмар» для розміщення і зберігання приватних даних є обережне ставлення до них самих розробників. За даними дослідження, здійсненого компанією Lieberman Software, більше половини (51%) IT-спеціалістів, що мають безпосередній стосунок до розробки та обслуговування «хмарних» сервісів, відмовляються зберігати в них свої особисті дані, а 86% – критично важливу корпоративну інформацію [8].

У листопаді 2012 р. зазначена компанія провела опитування учасників світового конгресу Cloud Security Alliance (CSA) і з'ясувала, що 88% з них вважають небезпечним зберігання даних у «хмарі» через високий ризик їх втрати та/або викрадення [9].

Немає сумніву, що як керівництво Євросоюзу, так і уряди держав-членів ЄС сповна усвідомлюють означені вище ризики та загрози. Ще у 2009 р. експерти Європейської агенції з телекомунікаційної та інформаційної безпеки (European Network and Information Security Agency – ENISA) відзначали: «Хмарні обчислення створюють для споживачів і провайдерів низку специфічних ризиків щодо захисту даних. Так, у деяких випадках споживачеві дуже складно проконтролювати, як саме і наскільки законно поводиться з його даними провайдер «хмарних» послуг. Ця проблема особливо загострюється у випадках множинних пересилок даних, наприклад, між інтегрованими хмарами» [10].

Отже, після цільового аналізу перелічених фахівцями НІСД ризиків постає нагальна необхідність з'ясувати, чи дійсно для України хмарні технології є настільки необхідними. У зв'язку з цим розглянемо насамперед, що саме нам пропонують народні депутати у вищевказаному законопроекті № 4302. Крім того, слід обговорити перспективи впровадження у діяльність Національного Банку України хмарних технологій, як про це було заявлено офіційним представником НБУ наприкінці 2012 р. і згодом повторено головою НБУ Валерією Гонтаревою у 2014 р. [12; 13].

За твердженням ініціаторів законопроекту № 4302, його прийняття сприятиме зміцненню співробітництва з Європейським Союзом щодо розвитку інформаційного суспільства.

Необхідність проходження усіма системами, в яких обробляється інформація, що належить до державних інформаційних ресурсів, подвійної процедури підтвердження відповідності є, на думку авторів законопроекту, застарілою, призводить до нераціонального використання державних ресурсів: «Так, не лише бюджетні кошти, а й значні людські ресурси, які в теперішніх умовах мали б бути спрямовані на захист державної таємниці, розпорошуються на захист відкритої та конфіденційної інформації, що не потребують застосування додаткових засобів захисту. Внаслідок згаданого також стримується і сам розвиток інформаційно-комунікаційних технологій в Україні, зокрема у сфері електронного урядування, освіти та науки» [11].

Крім того, використання систем хмарних обчислень начебто «сприятиме зменшенню витрат на побудову та розширення суб'єктами владних повноважень власних обчислювальних потужностей для ізольованої обробки і зберігання значного масиву інформації, з якою вони працюють. <…> Ізольованої обробки потребуватиме лише державна таємниця».

Перед нами типовий приклад застосування маніпулятивних технологій. З приводу наведених цитат щодо обґрунтування необхідності прийняття законопроекту № 4302 необхідно вказати такі моменти.

По-перше, як зауважують ініціатори розглядуваного законопроекту, бюджетні кошти та значні людські ресурси розпорошуються на захист відкритої та конфіденційної інформації.

Але згідно з ч. 1 ст. 20 Закону України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII за порядком доступу інформація поділяється на відкриту та інформацію з обмеженим доступом. Згідно з ч. 1 ст. 21 вказаного Закону та ч. 1 ст. 6 Закону України «Про доступ до публічної інформації» від 13 січня 2013 р. № 2939-VI інформацією з обмеженим доступом є конфіденційна, таємна та службова інформація.

В ч. 2 ст. 6 Закону України «Про доступ до публічної інформації» визначені причини обмеження доступу до конфіденційної, таємної та службової інформації. Отже, обмеження доступу до такої інформації здійснюється відповідно до закону тільки в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи злочинам, для охорони здоров'я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя.

До *конфіденційної* інформації, згідно з Законом України «Про інформацію», належить, зокрема, інформація про особу (персональні дані).

Слід нагадати, що згідно з ч. 1 ст. 1 Закону України «Про захист персональних даних» від 1 червня 2010 р. № 2297-VI цей Закон регулює правові відносини, пов'язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних. А згідно з ч. 1 ст. 8 вказаного Закону особисті немайнові права на персональні дані, які має кожна фізична особа, є невід'ємними і непорушними.

Також необхідно зазначити, що відповідно до ст. 3 Конституції України права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави.

Відповідно до ч. 1 ст. 8 Закону України «Про доступ до публічної інформації» *таємною* визнається інформація, яка містить державну, професійну, банківську таємницю, таємницю слідства та іншу передбачену законом таємницю. Крім того, наголошується на тому, що розголошення таємної інформації може завдати шкоди особі, суспільству і державі.

Згідно з ч. 1 ст. 9 Закону України «Про доступ до публічної інформації» до *службової* може належати інформація:

1) що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;

2) зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Отже, автори законопроекту № 4302 фактично пропонують відмовитись від положень ст. 3 Основного Закону України, а також від правових норм, що регламентують захист банківської таємниці, таємниці слідства, інформації, зібраної в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

У свою чергу, охороняти *належним чином* потрібно буде лише відомості, віднесені законом до державної таємниці. Всі інші види інформації з обмеженим доступом «не потре-

бують застосування додаткових засобів захисту» [11]. Подібні заяви від парламентарів, на нашу думку, є щонайменше необачними.

По-друге, «загальному державному курсу щодо дерегуляції», за логікою ініціаторів законопроекту № 4302, підлягає як інформаційна безпека держави, так і національна безпека загалом. Це означає передачу функцій щодо захисту інформації приватним (у тому числі іноземним) компаніям. З такою позицією не можна погодитись, адже її дотримання є фактично зрадою національних інтересів України.

Як було вказано вище, відповідно до норм розглядуваного законопроекту банківська таємниця також не потребує застосування додаткових засобів захисту. Це цілком узгоджується з позицією керівництва Національного банку України: «Нацбанк України планує перейти до хмарної моделі виробництва ІТ-сервісів. Про це повідомили в компанії DeNovo, яку обрали виконавцем проекту. <…> Під цей проект розроблена дорожня карта переходу, проведено обстеження та розроблена концепція трансформації ІТ-інфраструктури Нацбанку. Затверджена НБУ дорожня карта проектів передбачає віртуалізацію та оптимізацію ІТ-інфраструктури в короткостроковій перспективі і перехід до моделі хмарних обчислень – в середньостроковій» [12].

Наступне повідомлення про перспективи використання хмарних технологій в банківській системі України міститься в прес-релізі на офіційному сайті НБУ: «3 грудня 2014 р. в Національному банку України відбулася відкрита лекція на тему «Основні драйвери розвитку цифрового банкінгу у світі» одного із провідних світових експертів у галузі цифрового банкінгу Кріса Скіннера. Захід відбувся за участю Голови Національного банку України, керівників банків та освітніх установ, ІТ-спеціалістів банків та представників ЗМІ. На думку Кріса Скіннера, єдиний шлях виживання для банківської системи в умовах цифрової революції – це оцифровування послуг, мобільні додатки, використання «хмарних» технологій. <…> Голова Національного банку Валерія Гонтарева зазначила: «Майбутнє банківської системи – це широке використання цифрових послуг. <…> Досвід міжнародного ринку дає змогу нам правильно вибудувати пріоритети розвитку фінансового співтовариства. Сьогодні банківська система України переживає етап якісної трансформації і готова до переходу банків в еру цифрових технологій» [13].

Нарешті, слід зазначити, що Указом Президента України від 15 березня 2016 р. № 96/2016 було затверджено Стратегію кібербезпеки України, метою якої проголошено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Для досягнення цієї мети необхідним є, зокрема, забезпечення кіберзахисту державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, а також інформаційної інфраструктури, яка знаходиться під юрисдикцією України та порушення сталого функціонування якої матиме негативний вплив на стан національної безпеки і оборони України (критична інформаційна інфраструктура).

Несанкціоноване втручання в роботу об’єктів критичної інформаційної інфраструктури (в тому числі доступ до інформації, що міститиметься у «хмарах») може загрожувати економічній, екологічній, соціальній та іншим видам безпеки і призвести до таких наслідків:

– надзвичайна ситуація;

– блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об’єктів підвищеної небезпеки;

– блокування роботи державних органів, органів місцевого самоврядування;

– блокування діяльності військових формувань, органів військового управління, Збройних Сил України в цілому або втручання в автоматизовані системи керування зброєю;

– порушення безпечного функціонування банківської та/або фінансової системи держави;

– масові заворушення [14].

Висновки. Таким чином, враховуючи усі вищенаведені об’єктивні ризики використання хмарних технологій, однозначно можна стверджувати, що їх запровадження нега-

тивно позначиться на стані як інформаційної безпеки (складовою якої є кібербезпека), так і національної безпеки загалом.

Хмарні технології лише зашкодять цілісності об'єктів критичної інформаційної інфраструктури держави.

Список використаних джерел:

1. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

2. Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів «хмарного» обчислення): аналітична записка [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua.

3. Хмарні обчислення в дослідницькому університеті [Електронний ресурс]. – Режим доступу : http://www.cloud.kpi.ua/?page_id=132.

4. Офіційний сайт Microsoft [Електронний ресурс]. – Режим доступу : http://www.microsoft.com.

5. Перспективи розвитку ринку хмарних обчислень в Україні: переваги та ризики: аналітична записка [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua.

6. Working Paper on Cloud Computing – Privacy and data protection issues ("Sopot Memorandum"). International Working Group on Data Protection in Telecommunications 51st meeting, 23-24 April 2012, Sopot (Poland) [Електронний ресурс]. – Режим доступу : http://clck.ru/8aJ9c.

7. Мошеннические облачные сервисы – бич 77% компаний [Електронний ресурс]. – Режим доступу : http://www.securitylab.ru/news/436587.php.

8. IT-специалисты не спешат доверить свои данные «облаку» [Електронний ресурс]. – Режим доступу : http://www.hitech.newsru.com/article/14dec2012/cloudrisk.

9. Lieberman Software: «IT-специалисты не доверяют облачным сервисам» [Електронний ресурс]. – Режим доступу : http://www.securitylab.ru/news/435160.php.

10. Cloud Computing. Benefits, risks and recommendations for information security. European Network and Information Security Agency (ENISA). November, 2009 [Електронний ресурс]. – Режим доступу : http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment.

11. Про внесення змін до деяких законодавчих актів України щодо обробки інформації в системах хмарних обчислень : проект Закону України (реєстр. від 24 березня 2016 р. № 4302) [Електронний ресурс]. – Режим доступу : http://www.rada.gov.ua.

12. Нацбанк збирається перейти на «хмари» [Електронний ресурс]. – Режим доступу : http://www.epravda.com.ua/news/2012/12/12/350552

13. КрісСкіннер: «Майбутнє банківської системи України за новітніми технологіями» [Електронний ресурс]. – Режим доступу : http://www.bank.gov.ua/control/uk/publish/article?art_id=12504076.

14. Проект Стратегії забезпечення кібернетичної безпеки України [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua.