Федонюк С. В.
Східноєвропейський національний університет імені Лесі Українки,
м. Луцьк, Україна

ОСОБЛИВОСТІ РЕГУЛЮВАННЯ ТРАНСКОРДОННИХ СИСТЕМ «ХМАРНИХ ОБЧИСЛЕНЬ» У ЄВРОПЕЙСЬКОМУ СОЮЗІ

Нова стратегія Європейської комісії щодо розкриття потенціалу хмарних обчислень в Європі передбачає заходи, що забезпечать можливість створення додатково 2,5 млн. нових робочих місць та збільшити до 2020 р. ВВП ЄС на 160 млрд. євро (близько 1%)[4]. У такому вимірі «хмарні обчислення» розуміються як зберігання даних (такі як текстові файли, фотографії і відео) і програмного забезпечення на віддалених комп'ютерах, доступ до яких користувачі отримують доступ Інтернет. Реальні економічні вигоди вбачаються у широкому використанні хмарних рішень у бізнесі і державному секторі.

Як очікується, хмарні сервіси генеруватимуть у Європі майже 35 млрд євро доходів вже до 2014 р.[5]

В одній із семи флагманських ініціатив у рамках стратегії «Європа 2020», документі під назвою «Цифровий порядок денний для Європи» зазначено стратегічну ціль

---

[1] Лаптев И.Д. Актуальные проблемы формирования государственной информационной политики // Ежегодник 1998: государственная служба России. М., 1999. С. 182.
[2] Там же. С. 182.
[3] Засурский Я.Н. Информационное общество в России: парадоксы Интернета // Информационное общество. 2003. № 5. С. 205.
[4] Digital Agenda: New strategy to drive European business and government productivity via cloud computing. URL: http://europa.eu/ (дата обращения: 01.04.213).
[5] Digital Agenda: Commission seeks views on how best to exploit cloud computing in Europe. URL: http://europa.eu/ (дата обращения: 01.04.2013).

– «розвивати комунітарну стратегію щодо використаня хмарних обчислень, зокрема для потреб адміністрації та науки»[1].

У зв'язку із специфікою сервісів віддаленого доступу, які використовують міжнародні канали передачі даних і охоплюють користувачів як у різних країнах ЄС, так і за межами Союзу, передбачається великий транскордонний трафік даних у «хмарних» системах. «Хмарна» комунікація сприяє посиленню обміну даними з країнами що не входять до ЄС, або також Європейської економічної зони. А це вимагає застосування відповідних моделей регулювання.

Стратегія ЄС щодо упровадження та розвитку «хмарного» підходу передбачає дії у трьох областях[2]: розвиток правової бази, насамперед щодо захисту даних і приватності, прийняття норм і правил, які впливають на розгортання хмарних обчислень в державних і приватних організаціях; розвиток технологічної складової «хмарних» сервісів, посилення ролі Європейської комісії у технічній стандартизації програмних інтерфейсів і форматів даних, а також у розробці шаблонів договорів і угод щодо централізованого інформаційного обслуговування; розвиток ринку «хмарних» сервісів, підтримка експериментальних проектів, спрямованих на розгортання «хмарних» проектів через їх до фінансування через державні закупівлі у форматі взаємодії комунітарного, національного, а також регіонального, рівнів з метою вироблення спільних підходів до «хмарних» обчислень.

Головною проблемою у запровадженні «хмарних» технологій в системі державних комунікацій залишається питаня безпеки, що стосується передусім забезпечення конфіденційності персональних даних та доступу до іншої інформації з обмеженим доступом, а також охорона інтелектуальної власності. Так, директива 95/46/ЕС забороняє передачу персональної інформації з ЄЕЗ до країн, які не забезпечують належний рівень захисту (відповідно до ст. 25 і 26).

Що стосується захисту даних і безпеки інформації, то у контексті упровадження "хмарних» обчислень ці питання висвітлені рядом комюніке Європейської комісії, документами, що розроблені у рамках тзв. «Робочої групи статті 29» – Робочої групи із захисту осіб у зв'язку з обробкою персональних даних[3], створеної відповідно до ст. 29 Директиви ЄС (95/46/ЕС) про захист фізичних осіб стосовно обробки персональних даних та про вільний рух таких даних та звіті Європейського агентства безпеки мереж та інформації ENISA («Оцінка ризику хмарних обчислень»)[4].

Так, відповідно до ст. 13 (1) директиви 95/46/ЄС, держави-члени можуть обмежувати застосування деяких положень цієї директиви з питань національної та громадської безпеки чи кримінального переслідування та профілактики злочинності. Також, згідно із ст. 2 (d) і (e) зазначеної директиви вимагається розмежування й ідентифікація контролера й виконавця у системі постачання даних. Проте застосування «хмарного» підходу у багатьох випадках нівелює таке розмежування, оскільки державні інституції, фактично суб'єкти контролю, можуть виконувати також функції процесорів даних[5].

Також, згідно із ст. 17 директиви 95/46/ЄС, мають бути забезпечені цілісність і доступність даних, які є найважливішими елементами у наданні послуг «хмарних" обчислень. Відповідності до директиви, контролер і процесори повинні вжити технічних та організаційних заходів для захисту персональних даних від випадкового або

---

[1] A Digital Agenda for Europe (COM(2010) 245 final/2). – С. 26. URL: http://eur-lex.europa.eu/ (дата обращения: 01.04.2013).

[2] KroesNeelie. Towards a European Cloud Computing Strategy/ Neelie Kroes URL: http://europa.eu/ (дата обращения: 01.04.2013).

[3] «Working party on the Protection of Individuals with regard to the Processing of Personal Data».

[4] ENISA (2009) Cloud Computing Risk Assessment http://www.enisa.europa.eu/ (дата обращения: 01.04.2013).

[5] ENISA (2009) Cloud Computing Risk Assessment, pp 101. URL: http://www.enisa.europa.eu/ (дата обращения: 01.04.2013).

незаконного знищення чи випадкової втрати, зміни, несанкціонованого розкриття чи доступу. Проте досі в ЄС немає єдиних стандартів у цій галузі.

Крім того, поки що для систем «хмарної» комунікації не врегульовано питання суб'єкта фіксації порушень безпеки даних, як це передбачено ст. 4, 8, 13, 19 директиви щодо захисту персональних даних.

Окремо стоїть питання відповідальності провайдерів послуг, у випадку передавання чи приймання незаконної інформації що надана третьою стороною. У цьому сенсі діюча директива про електронну комерцію[1] дещо не відповідає вимогам хмарних моделей, оскільки провайдери у більшості випадків фактично не мають стосунку до незаконного контенту. Сьогодні онлайн-сервіси часто мігрують на хмарні інфраструктури, що полегшує можливість пропозиції більш інтегрованих послуг. А це призводить до формування більш складної системи правовідносин, що стало предметом відповідної ініціативи Єврокомісії, розробленої для подолання проблем, що пов'язані з фрагментацією норм і практик, що застосовуються в рамках ЄС та у відносинах із третіми країнами у зв'язку із ймовірним трафіком нелегального контенту й розміщення його в мережі[2]. У зв'язку з тим, що згадану вище директиву прийнято ще до появи «хмарних» провайдерів, їх місце в інфраструктурі трансферу контенту часто не означено конкретно, внаслідок чого мають місце різні трактування в прецедентному праві країн ЄС з точки зору стосунку до нелегального контенту (наприклад, принципово різні з точки зору дії директиви рішення щодо сервісу із почасти сумнівним контентом «Pirate Bay» в Італії та Швеції[3,4]).

Питання безпеки пов'язане також з необхідністю упровадження безпечних методів електронної аутентифікації для здійснення «хмарних» операцій, зокрема – прийняття загальних стандартів, які дозволяють безпечне й водночас безшовне використання послуг, що вимагають надійної аутентифікації і авторизації у системах хмарних обчислень. У цьому зв'язку варто відмітити прийняття у червні 2012 р. пропозиції Єврокомісії щодо електронної ідентифікації та аутентифікації, яка враховує особливості «хмарних» моделей[5]. У рамках нової системи для електронної ідентифікації та електронних послуг довіри буде: забезпечити взаємне визнання і прийняття електронної ідентифікації у транскордонних системах; надання юридичної сили і взаємного визнання послуг, включаючи зміцнення діючих правил щодо електронного підпису та забезпечення правової основи для електронних печаток і часових штампів, електронної акцептації документа, електронної доставки та перевірки автентичності веб-сайту.

Фактично сьогодні відбувається адаптація норм що діють в ЄС до вимог часу, пов'язаних із стратегічною перспективою упровадження «хмарних» моделей.