УДК (004.75+004.056).000.34

**ГЛАДКІВСЬКА О.В.,** *кандидат фізико-математичних наук,*
*старший науковий співробітник,*
НДІІП НАПрН України

# ВПЛИВ ХМАРНИХ ТЕХНОЛОГІЙ НА СТАН ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ПРАВОВИЙ АСПЕКТ

***Анотація.*** *Про юридичний аспект проблем інформаційної безпеки, пов’язаних із впровадженням хмарних технологій.*

***Ключові слова:*** *інформаційні технології, хмарні технології, інформаційна безпека, , персональні дані, захист інформації в “хмарі”.*

***Аннотация.*** *О юридическом аспекте проблем информационной безопасности, связанных с внедрением облачных технологий.*

***Ключевые слова:*** *информационные технологии, облачные технологии, информационная безопасность, персональные данные, защита информации в “облаке”.*

***Summary.*** *About a legal aspect of information security issues related to implementation of cloud technologies.*

***Keywords****: information technology, cloud computing, information security, personal data, security of information in cloud computing.*

***Постановка проблеми.*** В сучасних умовах, поряд з кроками в напрямку розвитку інформаційного суспільства, важливими є питання його захисту, захисту інформаційної безпеки та інформаційних національних інтересів України.

Для розвитку інформаційного суспільства характерне поєднання глобальних інформаційно-комунікаційних систем, інтеграція баз даних та знань, зростання спектру послуг і сервісів, різке збільшення клієнтського навантаження на серверний простір. Результатом еволюційного розвитку інформаційних технологій (далі – ІТ) за останнє десятиліття стали *cloud computing* – “хмарні технології” (обчислення). За допомогою їх впровадження стає можливим вирішення виниклого протиріччя – невідповідності між бурхливим зростанням обсягів інформаційних потоків і мережевих сервісів та сучасним технічним станом програмно-апаратного забезпечення мережевої інфраструктури інформаційних систем. Під час використання хмарних технологій програмне та технічне забезпечення надається користувачеві як Інтернет-сервіс; він має доступ лише до власних даних, а не до інфраструктури, операційної системи і програмного забезпечення, з якими працює. “Хмара” – це Інтернет, який приховує усі технічні деталі.

Інтенсивне освоєння хмарних технологій ІТ-компаніями, застосування у малому та середньому бізнесі, у навчальному процесі, для управління підприємствами, перехід на хмарні технології ІТ-інфраструктур державних органів – все це свідчить про черговий якісний стрибок у галузі інформаційних технологій. З іншого боку, як вказано в [1], “важливе рішення щодо використання cloud computing несе в собі реальні й перспективні загрози безпеки бізнесам, якими вони керують, і це може розглядатися, як новий технологічний, економічний, фінансовий і безпековий виклик початку XXI ст.”.

Дослідження теоретичних і практичних засад функціонування хмарних сервісів, і, зокрема, інформаційної безпеки хмарних сервісів, набули достатнього поширення у науці, особливо в частині програмного та технічного забезпечення. Однак, нормативне регулювання відносин стосовно хмарних технологій є менш дослідженою сферою.

Поряд з перевагами хмарних обчислень мова йде і про ризики, з якими пов’язаний перехід на “хмари”, найістотніший з яких – загроза інформаційній безпеці. Відповідно, основними правовими проблемами, що пов’язані з використанням хмарних обчислень, є забезпечення інформаційної безпеки та захист персональних даних у віртуальному середовищі. Ці важливі проблеми стосуються дотримання конституційних принципів, соціальних проблем, захисту національної безпеки. Важливість та актуальність дослідження випливає і з того, що нормативно-правова база “відстає” від темпів розвитку ІТ-сфери (і, зокрема, хмарних технологій).

*Аналіз останніх досліджень*. Поточний стан і перспективи глобального розвитку хмарних технологій та сервісів, а також аналіз особливостей та динаміки хмарного ринку в Україні наведено в [2]. Порівняльний аналіз сучасних моделей побудови, обслуговування та сервісу хмарних технологій проведено в [3]. Дослідження [4] стосується аналізу програмного забезпечення різних постачальників, яке реалізує технологію “хмарних обчислень”. Про хмарні технології безпеки – ефективні методи поєднання антивірусного програмного забезпечення з хмарною технологією (хмарні антивіруси) йдеться в роботі [5].

В дослідженні [6] охарактеризовано технологію хмарних сервісів, проаналізовано основні задачі і принципи її інформаційної безпеки, визначено перспективи розвитку як самої технології, так і параметрів безпеки.

Слід вказати й на роботу [7], в котрій розглядається сучасний стан застосування та розвитку хмарних обчислень, основні переваги та недоліки їх використання на рівні держави, на підприємствах та в науковій діяльності. Визначаються та аналізуються стандарти, нормативні та керівні документи в галузі інформаційної безпеки хмарних обчислень, що розроблені Національним інститутом стандартів і технологій США (NIST), Європейським агентством мережевої та інформаційної безпеки (ENISA) і Альянсом безпека в хмарі (Cloud Security Alliance, CSA), а також наводяться результати детального аналізу питань інформаційної безпеки в хмарі. Огляд діючих та розроблюваних міжнародних стандартів, що стосуються хмарних технологій (обчислень), наведено, наприклад, в [8]. Аналіз застосування хмарних технологій у системі електронного урядування здійснено в [9] та в ін.

В [1] проаналізовано виникнення нового технологічного мегатренду *“cloud computing”*, зокрема, досліджено сам термін. Автор наводить різні варіанти перекладу (“хмарні обчислення”, “хмарові обчислення”, “обчислення у хмарах” та ін.) і вказує, що “цей термін поки що не знайшов остаточного наукового перекладу в українській науці”. Ще можна додати сюди використання терміну “хмаринні технології” в [10, с. 5].

Питання правового регулювання сфери хмарних технологій розглядаються також в роботах [2 – 7].

***Метою статті*** є спроба ідентифікації основних правових проблем, пов’язаних з використанням хмарних технологій (обчислень), зокрема, щодо їх впливу на інформаційну безпеку.

***Виклад основного матеріалу.*** Згідно з визначенням NIST [15, с. 2], хмарні технології (англ. *cloud computing*) – це модель забезпечення повсюдного та зручного доступу на вимогу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних,

прикладних програм та сервісів), і які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера. Іншими словами, основне завдання хмарних технологій – надання користувачам якісних послуг з гарантованою якістю за умов збереження цілісності, доступності та конфіденційності інформаційних ресурсів. Слід зазначити, що визначення поняття “хмарні” технології (обчислення), основні моделі розгортання “хмарних” сервісів та моделі сервісу “хмарних” технологій (обчислень) наводяться та аналізуються в численних публікаціях, тому в даному дослідженні не будемо зупинятись на роз’ясненні вказаних понять.

На сьогодні світовими провідними організаціями, що займаються питаннями безпеки в хмарі, є CSA, ENISA і NIST. Кожна з організацій створила відповідний документ з класифікацією всіх існуючих проблем інформаційної безпеки в хмарі. В Таблиці 1 наведено порівняння правових складових інформаційної безпеки (далі – ІБ) в класифікаціях названих організацій, а в Таблиці 2 – організаційних складових ІБ.

Таблиця 1

**Порівняння правових складових ІБ в класифікаціях CSA, ENISA та NIST** [7]

| № | Правові питання ІБ | Класифікація | | |
|---|---|---|---|---|
| | | CSA | ENISA | NIST |
| 1 | Дотримання міжнародних та державних стандартів, законів і правил | + | + | + |
| 2 | Договір між постачальником та клієнтом | + | + | + |
| 3 | Право власності на електронні дані | + | + | + |
| 4 | Невідповідність законодавств різних держав у сфері електронних даних | + | + | + |
| 5 | Захист авторських прав | + | – | – |
| 6 | Дотримання законів та правил держав до даних у хмарі | + | + | + |
| 7 | Зміна постачальника послуг, або його купівля іншим постачальником | + | + | + |

Таблиця 2

**Порівняння організаційних складових ІБ в класифікаціях CSA, ENISA та NIST [7]**

| № | Організаційні питання ІБ | Класифікація | | |
|---|---|---|---|---|
| | | CSA | ENISA | NIST |
| 1 | Управління ризиками (корпоративними, підприємства, інформаційними, постачальника послуг) | + | + | + |
| 2 | Управління безпекою інформації користувача | + | + | + |
| 3 | Довіра до постачальника послуг (проведення аудиту, тестування, оновлення забезпечення, підтримка в проведенні експертизи) | + | + | + |
| 4 | Захист від інсайдерів | + | + | + |
| 5 | Реагування на інциденти ІБ, їх моніторинг, вирішення | + | + | + |
| 6 | Захист персональних даних користувача | – | – | + |
| 7 | Управління авторськими правами | + | + | + |
| 8 | Відмова сервісів хмари по причині стихійного лиха, збоїв у роботі сервісів хмари, що підтримуються третьою стороною | + | + | + |

Більшість з проблем захисту інформації користувача в “хмарі” можна вирішити шляхом використання існуючих методів криптографічного захисту інформації, адміністративних заходів з боку як постачальника хмарних послуг, так і користувача, укладання договорів на надання послуг, які б враховували індивідуальні потреби клієнтів, прийняття міжнародних стандартів у галузі, введення контролю з боку держави та створення незалежних експертів у цій галузі [7].

Використання хмарних сервісів суттєво змінило підхід користувача до роботи з інформацією та програмами. Хмарні системи дозволяють мати доступ до інформації та серверів з будь-якого місця світу, звільнивши користувачів від необхідності мати стаціонарний комп’ютер та зробивши доступнішою спільну роботу багатьох людей, які можуть знаходитися в різних місцях. І ця обставина, пов’язана з архітектурою “хмари”, призводить до об’єктивних проблем забезпечення інформаційної безпеки.

Такими об’єктивними, невирішеними остаточно проблемами, пов’язаними з дотриманням безпеки персональних даних у “хмарах”, є [11]:

– безпека як така, тобто принципова здатність сервісів гарантувати зберігання та обробку даних згідно з законом;

– фізичне розміщення персональних даних та їх транскордонна передача, оскільки утримання дата-центру у будь-якій вигідній провайдеру точці Землі повністю відповідає самій ідеї “хмари”, але може бути небезпечним для користувача;

– доступ користувача до своїх персональних даних, оскільки об'єктивно не він контролює цей доступ.

Основними напрямками ризиків для безпеки даних вважають наступні:

1) нормативно-правовий (конфлікт юрисдикцій в частині регулювання транскордонної передачі даних та обмежень щодо їх захисту);

2) технологічний (ситуації, коли надмірна віддаленість сервера може призвести до затримок транспортування даних і критичних помилок у роботі програм, а також коли один потужний дата-центр обслуговує велику кількість споживачів по всьому світу).

У матеріалах 2012 р. міжнародної команди експертів з захисту персональних даних у телекомунікаційних мережах виділено такі проблеми та ризики використання “хмар”:

- технологія все ще у стадії розроблення і не апробована остаточно;

- досі нема міжнародної угоди про єдину термінологію, хоча технологія є транскордонною, а обробка даних фактично стала глобальним процесом;

- діяльність провайдерів є недостатньо прозорою і не може бути повністю відслідкована. Це значно ускладнює оцінку ризиків і створення єдиних правил гри; 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.

З метою створення умов для безперешкодного застосування хмарних обчислень, держави сформулювали перелік питань, на які слід знайти відповіді [16]:

– Захист даних після закінчення договору.

– Конфіденційність та цілісність даних.

– Місцезнаходження та передача даних.

– Володіння даними.

– Пряма та непряма відповідальність за послугу з боку провайдера послуг та підрядників.

– Навчання користувачів та організацій принципам роботи з хмарними послугами.

– Оновлення нормативної бази у сфері державних закупівель.

– Стандартизація та сертифікація у сфері постачання хмарних послуг.

– Сприяння розвитку інноваційних ІТ-компаній, які використовують нові технології для створення програмного забезпечення.

У зв’язку з тим, що для хмарних технологій стратегічним питанням є обрання розташування дата-центрів, то найчастіше такі центри розміщені в офшорних юрисдикціях або в зонах з певною географічною особливістю, і нерідко у країнах з недосконалим законодавством у сфері кіберзахисту та захисту персональних даних. Наприклад, дата-центри корпорації Google розташовані не тільки в США, але й у багатьох країнах світу [17]. У 2009 р. корпорація отримала патент на дата-центр морського базування з розміщенням на судні, котре перебуває в нейтральних водах. Таким чином цей об’єкт виведено за межі юрисдикції будь-якої держави світу, і не треба буде платити податки. Але стратегічно важливішим є те, що для вирішення частини проблем забезпечення інформаційної безпеки можна розмістити на морській платформі резервний дата-центр на випадок стихійного лиха.

Зазначимо, що для дата-центрів, які обслуговують органи державної влади США, діє норма, що унеможливлює їх розміщення поза територією держави. А от Держдума РФ у липні 2014 р. прийняла закон про персональні дані, що зобов’язує зарубіжні інтернет-компанії зберігати особисту інформацію про російських користувачів тільки на серверах, розміщених на території Росії. Передбачається, що цей закон буде введено в дію у 2016 році.

Функціонування хмарних технологій потребує регуляції багатьох галузей права, зокрема через законодавство про захист персональних даних. Закон України “Про захист персональних даних” містить більшість положень конвенції Ради Європи про захист осіб у зв’язку з автоматизованою обробкою персональних даних, що розширює можливості використання новітніх технологій. Застосовуючи хмарні технології, слід також враховувати особливості регулювання безпеки персональних даних у різних галузях, тому що різні стандарти існують у банківському секторі, страхуванні, системі охорони здоров’я, у сфері надання освітніх послуг та ін. Якщо виникає питання, як захищати персональні дані, якщо на клієнта поширюється одна юрисдикція, а на компанію – постачальника інформаційних послуг – інша, то, як правило, постачальники хмарних послуг застосовують законодавство тієї держави, де розташований дата-центр.

Важливою правовою проблемою, пов’язаною з такою особливістю застосування хмарних технологій як питання юрисдикції, є розподіл відповідальності. Хмарні обчислення в рамках моделей приватної, спільної, публічної або гібридної хмари “створюють нову динаміку у відносинах між організацією та її інформацією у зв’язку з наявністю третьої сторони – постачальника хмари. Це створює нові труднощі у розумінні, як застосовувати закон у великій різноманітності нових сценаріїв управління інформацією” [13]. Безумовно, розподілити відповідальність між великою кількістю суб’єктів, які можуть бути під різними юрисдикціями, в умовах невизначеності, коли невідомо хто, де, за що буде нести відповідальність, і за яким законодавством – це складне питання.

Таким чином, завдяки особливостям свого функціонування хмарні сервіси утворюють цілком специфічне середовище, в якому традиційні нормативно-правові

механізми, практики та підходи стають здебільшого неефективними. У будь-якому випадку слід дотримуватись “золотого” правила, вказаного в [13]: “Незалежно від використовуваної моделі обчислень – хмарної чи ні – потрібно враховувати питання законодавства, особливо стосовно даних, які ви збираєте, зберігаєте та обробляєте”.

На урядовому рівні усвідомлюють, що настала пора “вдосконалення нормативно-правового забезпечення та попередження й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері” [18], що “неврахування …технологічних тенденцій розвитку сфери ІКТ, особливо таких як “мобільність”, “соціалізація”, “хмаринні технології” та “обробка великих даних”, і високих темпів їх розвитку може призвести до критичного відставання України від країн-лідерів” [10].

Так, 1 травня 2014 року введено в дію важливий Указ Президента України № 449/2014 “Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” [18]. Зокрема, в заходах передбачається розробити проекти Стратегії розвитку інформаційного простору України та Стратегії кібернетичної безпеки України, нової редакції Доктрини інформаційної безпеки України, Закону України про кібернетичну безпеку України.

У Рекомендаціях парламентських слухань на тему “Законодавче забезпечення розвитку інформаційного суспільства в Україні”, що відбулися 18 червня 2014 року, зазначено: “У переліку пріоритетів стратегічного розвитку України особливе місце повинні займати захист прав, свобод і безпеки громадян в інформаційній сфері, відмова від ідей тотального інформаційного контролю та розвиток інноваційних галузей економіки, зокрема вітчизняної індустрії інформаційних технологій, надання послуг та виробництво програмної продукції”, вказано на необхідність “Верховній Раді України: законодавчо визначити засади державної політики щодо забезпечення інформаційної безпеки України як однієї з основних конституційно визначених функцій держави; Кабінету Міністрів України: сформувати ефективну систему забезпечення інформаційної безпеки України та її складової – кібернетичної безпеки” [19].

З 1 січня 2014 року вступив в силу Закон України “Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних” від 03.07.13 р. № 383-VII. Цим законом передбачена суттєва модернізація всієї галузевої нормативно-правової бази, зокрема, переглянуто саму процедуру реєстрації баз даних. Якщо раніше передбачалась їх безумовна та обов‘язкова реєстрація, то тепер “володілець персональних даних повідомляє Уповноваженого про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних” [20], згідно відповідного переліку, що встановлюється Уповноваженим. В [21] даються наступні роз’яснення: “…Обробкою персональних даних, що становить особливий ризик для прав і свобод суб’єктів, є будь-яка дія або сукупність дій, а саме збирання, реєстрація, накопичення, зберігання, адаптування, зміна, поновлення, використання і поширення (розповсюдження, реалізація, передача), знеособлення, знищення, у тому числі з використанням інформаційних (автоматизованих) систем…”.

У поточному році Верховна Рада України прийняла ще такі закони стосовно інформаційної сфери:

– “Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Закону України “Про інформацію” та Закону України “Про доступ до публічної інформації” від 27.03.14 р. № 1170-VII (закон передбачає внесення змін у чотири Кодекси і 53-и Закони України).

– “Про стандартизацію” від 05.06.14 р. № 1315-VII.

– “Про метрологію та метрологічну діяльність” від 05.06.14 р. № 1314-VII.

– “Про внесення змін до Закону України “Про видавничу справу” від 01.07.14 р. № 1554-VII.

– “Про внесення змін до Закону України “Про рекламу” від 05.06.14 р. № 1322-VII.

Були прийняті й деякі інші важливі документи:

– Постанова Верховна Рада України “Про прийняття за основу проекту Закону України про електронну комерцію” від 03.06.14 р. № 1298-VII.

– Наказ Уповноваженого Верховної Ради України з прав людини “Про затвердження документів у сфері захисту персональних даних” від 08.01.14 р. № 1/02-14, яким затверджено такі документи:

1. Типовий порядок обробки персональних даних.

2. Порядок здійснення Уповноваженим Верховної Ради України з прав людини контролю за додержанням законодавства про захист персональних даних.

Порядок повідомлення Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, яка становить особливий ризик для прав і свобод суб’єктів персональних даних, про структурний підрозділ або відповідальну особу, що організовує роботу, пов’язану із захистом персональних даних при їх обробці, а також оприлюднення вказаної інформації.

– Наказ Міністерства юстиції України “Про систему обліку публічної інформації в Міністерстві юстиції України та його територіальних органах” від 28.05.14 р. № 846/5.

– Наказ Міністерства юстиції України, Адміністрації Державної служби спеціального зв’язку та захисту інформації України “Про внесення зміни до Вимог до формату посиленого сертифіката відкритого ключа” від 05.06.14 р. № 873/5/269.

– Наказ Міністерства економічного розвитку і торгівлі України “Про порядок складання та подання запитів на одержання публічної інформації в Державній інспекції України з контролю за цінами від 19.05.14 р. № 555”.

– Наказ Міністерства охорони здоров’я України “Перелік відомостей, що містять службову інформацію, розпорядником якої є Міністерство охорони здоров’я України” від 06.05.14 р. № 299.

– Наказ Міністерства охорони здоров’я України ”Про організацію виконання Закону України “Про доступ до публічної інформації” у Міністерстві охорони здоров’я України” від 06.05.14 р. № 299.

– Наказ Служби безпеки України “Про затвердження змін до деяких нормативно-правових актів Служби безпеки України з питань провадження господарської діяльності з розроблення, виготовлення спеціальних технічних засобів для зняття інформації з каналів зв’язку, інших засобів негласного отримання інформації, торгівлі спеціальними технічними засобами для зняття інформації з каналів зв’язку, іншими засобами негласного отримання інформації” від 30.04.14 р. № 212.

– Наказ Адміністрації Державної служби спеціального зв’язку та захисту інформації України “Інструкція про приймання, передавання, доставку та зберігання криптограм” від 22.04.14 р. № 195.

***Висновки.***

Здійснений аналіз наведених нормативно-правових актів, а також наукових публікацій за темою дослідження дозволяє стверджувати наступне.

У світовій практиці відсутнє спеціальне правове регулювання хмарних технологій (обчислень).

Впровадження хмарних технологій відбувається насамперед там, де вигода є найбільшою, тобто проекти не передбачають одночасного і повсюдного переходу до нової моделі.

Хмарні сервіси зберігання даних мають відповідати як встановленим вимогам безпеки, так і нормам законодавства.

Забезпечення інформаційної безпеки має здійснюватись одночасно із впровадженням чи використанням інформаційних технологій, проте українське законодавство поки що не приділяє хмарним технологіям особливої уваги, нормативно-правова база “відстає” від темпів розвитку ІТ-сфери.

В Україні відсутні національні стандарти, що встановлюють належні вимоги до якості та надійності хмарних технологій і послуг.

Потрібно не просто розробити правову модель використання нової технології, а й розподілити відносини між користувачами та постачальниками, забезпечивши найбільш розумний баланс між їхніми інтересами.

Шляхи вдосконалення правового регулювання застосування та впровадження новітніх інформаційних технологій, в т. ч. хмарних технологій (обчислень), у довгостроковій перспективі вказано в:

Указі Президента України від 28.04.14 р. № 449/2014 “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” [18];

Рекомендаціях парламентських слухань на тему “Законодавче забезпечення розвитку інформаційного суспільства в Україні”, що відбулися 18.06.14 р. [19];

Програмі розвитку сфери інформаційно-комунікаційних технологій в Україні [10].

Розроблення та прийняття названих документів є значним кроком на шляху вироблення державою ефективної регуляторної політики у вказаному напрямку. Приймаючи національні програми, слід, за можливості, якнайменше змінювати чинні правові засади. Зняти наявні бар’єри для розвитку хмарних технологій дозволить внесення окремих точкових поправок, які обов’язково мають узгоджуватися з базовими принципами законодавства України.

Що стосується короткострокової перспективи, то конкретні кроки слід розпочинати із удосконалення нормативно-правової бази, зокрема, з визначення кібернетичної безпеки самостійною сферою національної безпеки, уточнення терміна “критична інфраструктура” та ін. На часі удосконалення спеціальних методик для використання хмарних технологій (обчислень) в органах державної влади й державних установах, аналіз договірних відносин між провайдером хмарних технологій (обчислень) та користувачем і т.п.

А поки що оптимізм вселяє думка фахівців з Microsoft, що “існуючі сьогодні правові проблеми типові для будь-якої нової технології і згодом юридичні перешкоди для хмарних обчислень перестануть існувати просто в силу природного розвитку ринку” [6].

*Подальші дослідження* будуть спрямовані на поглиблений аналіз стану нормативно-правової бази України щодо інформаційної безпеки та її складової – кібернетичної безпеки.

## Використана література

1. Зернецька О. Новий виток конкурентної боротьби в Інтернеті : Cloudcomputing // Інтернет-холдинг Олега Соскіна. – Режим доступу : http://soskin.info/ea/2011/9-10/201126.html

2. Гнатюк С. Перспективи розвитку ринку хмарних обчислень в Україні : переваги та ризики : аналітична записка. – Режим доступу : //www.niss.gov.ua/articles /1191

3. Юдін О.К., Зюбіна Р.В. , Зюбін Т.В. Сучасні моделі корпоративних мереж на базі хмарних технологій. – Режим доступу : //www.rusnauka.com/1_NIO_2014/Informatica/4_155702.doc.htm

4. Яковицький І. Технологія хмарних обчислень як інструмент створення інформаційної інфраструктури управління // Комунальне господарство міст. – 2012. – № 102. – С. 320-327.

5. Комiссар Д.О., Луппол Є.Ю. Хмарні технології безпеки. // Вісник східноукраїнського національного університету імені Володимира Даля. – 2013. – Ч. 1. – № 15(204). – С. 83-87.

6. Гудзовата О.О. Інформаційна безпека хмарних сервісів // Науковий вісник Львівського державного університету внутрішніх справ (серія економічна). – 2013. – № 2. – С. 228-239.

7. Аулов І.Ф., Горбенко І.Д. Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі // Прикладная радиоэлектроника. – 2013. – Т. 12. – № 2. – С. 194-201.

8. Міжнародний досвід. – Режим доступу : http://zpd.gov.ua/dszpd/uk/publish/article/53913sessionid=ABF5CECA F86F57E8E8E4B04651C56EDB. – (Сайт Державної служби України з питань захисту персональних даних).

9. Федонюк С.В. Хмарні технології в електронному врядуванні // Науковий вісник Волинського національного університету імені Лесі Українки (міжнародні відносини). – 2011. – № 20. – С. 13-19.

10. Програма розвитку сфери інформаційно-комунікаційних технологій в Україні. – Режим доступу : http://dknii.gov.ua/?q=node/1666. – (Сайт Державного агентства з питань науки, інновацій та інформатизації України).

11. Гнатюк С.Л. Актуальні питання захисту персональних даних у віртуальному середовищі (на прикладі технологій та сервісів хмарного обчислення). – Режим доступу : //www.uipdp.com/articles/2013-04/05.html

12. Прокопович О. Облачные технологи : понятие, правовое регулирование, зарубежный опыт // Закон и бизнес. – 2014. – №18-19 (1160-1161). – (по матер. VII ежегодной конференции корпоративных юристов (юрисконсультов), г. Киев, 25 апреля 2014 года). – Режим доступа : http://zib.com.ua/ru/print/84528-akuyu_strategiyu_izbrat_yuristu_dlya_borbi_s_prizvolom_chin.html

13. Уинклер Дж. Р. Облачные вычисления. Вопросы права и требований регулирующих органов. – Режим доступа : http://technet.microsoft.com/ru-ru/magazine/hh9 94647.aspx

14. Войниканис Е.О концепции правового регулирования облачных вичислений. – Режим доступа : http://easier.pro/news/legal/on_the_concept_of_legal_regula tion _of_cloud_computing

15. Mell P. The NIST Definition of Cloud Computing (Special Publication 800-145) : Recommendations of the National Institute of Standards and Technology / Peter Mell, Timothy Grance / National Institute of Standards and Technology, U.S. Department of Commerce. – September 2011. – 7 P. – Acces mode : http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

16. Каріченський О.В. Досвід та переваги використання технологій хмарних обчислень у державних проектах : материали Міжнар. наук. конгресу [“Інформаційне суспільство в Україні”], (Київ, 29 жовтня 2013 р.). – С. 41-42. – Режим доступу : http://congress.ogp.gov.ua/sites/default/files/Congress_2013-p1%20p2(1).pdf

17. Внутри Интернета. Как выглядят дата-центры Google. – Режим доступа : http://fishki.net/1302522-vnutri-interneta-kak-vygljadjat-data-centry-google.html

18. Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” : Указ Президента України від 01.05.14 р. № 449/2014. – Режим доступу : //www.prezident.gov.ua/documents/17588.html

19. Про Рекомендації парламентських слухань на тему: “Законодавче забезпечення розвитку інформаційного суспільства в Україні” : Постанова Верховної Ради України від 03.07.14 р. № 1565-VII // Відомості Верховної Ради України. – 2014. – № 33. – Ст. 1163. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1565-18/print1393204327402471#n12

20. Про внесення змін до деяких законодавчих актів України у зв’язку з прийняттям Закону України “Про інформацію” та Закону України “Про доступ до публічної інформації” : Закон України від 27.03.14 р. № 1170-VII // Відомості Верховної Ради України. – 2014. – № 22. – Ст. 816. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/1170-18/page

21. Лист Уповноваженого Верховної Ради України з прав людини (щодо захисту персональних даних) від 03.03.14 р. № 2/9-227067.14-1/НД-129. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/v7067715-14

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~