NETWORK AND APPLICATION SECURITY

DOI 10.20535/2411-1031.2019.7.2.190565
УДК 004.056.53

АРТЕМ ЖИЛІН,
АНДРІЙ ДІВІЦЬКИЙ,
АННА КОЗАЧОК

ПРОБЛЕМАТИКА ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ПРИ ВИКОРИСТАННІ ХМАРНИХ ТЕХНОЛОГІЙ

Запропоновано рішення завдання щодо створення захищених дата-центрів збереження інформації і відомостей державних електронних інформаційних ресурсів шляхом використання хмарних технологій. При цьому вітчизняні нормативно-правові акти не вирішують задачу забезпечення безпеки інформації при її віддаленій обробці в дата-центрах з використанням хмарних технологій, тому аналізується досвід міжнародних, національних стандартів та найкращих практик у цій сфері. Метою ж статті визначено аналізування проблематики захисту інформаційних ресурсів при використанні хмарних технологій. Для досягнення сформованої мети аналізуються технології хмарних обчислень та виконується порівняльний аналіз нормативно-правових документів щодо захисту інформації при використанні хмарних технологій. Надається визначення та характеристики хмарних обчислень, які відрізняють їх від інших типів обчислень, а саме самообслуговування на вимогу, об'єднання ресурсів, миттєва еластичність ресурсів, вимірюваний сервіс. Надається класифікація та приводиться аналіз організацій та органів, які розробляють нормативно-правові документи для хмарних обчислень. Вони створюють міжнародні стандарти і мають наступну ієрархію рівнів: міжнародний (ISO/IEC), міждержавний (форуми і консорціуми (Cisco, CSA)), регіональний (європейські органи ETSI, CEN / CENELEC), національний (закони та державні стандарти, відомчі нормативні документи, керівництва, інструкції, наприклад: (NIST). Також зазначається велика роль консорціумів в стандартизації та розвитку як самих хмарних технологій так і проблематики захисту інформації при їх використанні. Надається опис цих консорціумів та напрямків їх діяльності, виокремлюються та розглядаються документи, що були ними створені в сфері забезпечення безпеки хмарних технологій. Так розглядаються та порівняються ISO 17788, NIST SP 500-299, Керівництво з безпеки для критично важливих областей хмарних обчислень CSA та проекті ГОСТ Р "Захист інформації. Вимоги щодо захисту інформації, що обробляється з використанням технологій "марних обчислень". Основні положення". На основі проведеного аналізу документів представлено відображеність моделей послуг у нормативно-правових документах та зведені дані щодо наявних в документах методів захисту інформації в сфері хмарних обчислень.

Ключові слова: хмарні технології, хмарні сховища, інформаційна безпека, моделі послуг, стандарти, методи захисту інформації.

Постановка проблеми. Відповідно до Указу Президента України № 32/2017 "Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації" [1] поставлено завдання щодо створення захищених дата-центрів збереження інформації і відомостей державних електронних інформаційних ресурсів. Найбільш перспективним напрямом вирішення цього завдання є їх створення на основі використання хмарних технологій, що є сукупністю хмарних сховищ та хмарних обчислень (з англ. Cloud Computing) як технології оброблення даних в цих сховищах. В той же час вітчизняні нормативно-правові акти [2] не вирішують

задачу забезпечення безпеки інформації при її віддаленій обробці в дата-центрах з використанням хмарних технологій, натомість існує досвід інших міжнародних, національних стандартів та найкращих практик у цій сфері.

Багато стандартів, які сьогодні вимушено застосовуються для організації захисту інформації при хмарних обчисленнях, розроблено для "дохмарних" технологій таких як веб, платіжні системи, автоматизовані системи. Тому активно розроблюються стандарти і керівництва, що призначені для організації захисту хмарних обчислень [3]. Для сфери хмарних обчислень особливу роль відіграють міжнародні стандарти, оскільки споживачі і провайдери хмарних послуг часто знаходяться в різних країнах. Зважаючи на це обумовлюється актуальність проблеми встановлення вимог до захисту інформаційних ресурсів при хмарних обчисленнях.

Аналіз останніх досліджень і публікацій. Проведемо аналіз останніх вітчизняних та міжнародних публікацій, в яких розглядалася тематика захисту інформації у хмарних сховищах. Так в [4] зазначено, що багато завдань зі захисту інформації в хмарі може вирішуватися за допомогою існуючих методів криптографічного захисту інформації, адміністративних заходів з боку постачальника хмарних послуг, прийнятті міжнародних стандартів у галузі хмарних обчислень та введення контролю з боку держави. Наприклад в [5], для забезпечення конфіденційності та цілісності даних, що зберігаються в хмарі, пропонується використовувати алгоритми цифрового підпису та шифрування, які засновані на міжнародних стандартах, а для запобігання несанкціонованого використання профілю користувача – існуючі методи двофакторної автентифікації. Також в [5] зазначається, що більшість постачальників мають свій власний, іноді навіть добре документований інтерфейс для програмування, але це призводить до неможливості переходу користувачів від одного постачальника послуг до іншого. В [5], [6] також криптографія визначаються, як основний метод захисту та зауважується, що ефективне рішення із забезпечення захисту інформації в хмарній інфраструктури повинно включати: 1) закритий доступ до даних – необхідно забезпечити надійне управління ключами шифрування; 2) політики доступу – тільки авторизовані користувачі повинні мати доступ до конфіденційної інформації; 3) інтелектуальну систему, яка повинна збирати інформацію для аналізу поведінки користувачів і сповіщати у разі виявлення підозрілої активності.

Окрім цього, на практиці відомі методи реалізації механізмів захисту хмарних сховищ [7]. Так у вітчизняного провайдера хмарних сховищ "DENOVO" хмарна послуга G-cloud створена для задоволення потреб підприємств, що потребують при експлуатації своїх систем наявності сертифікату КСЗІ (комплексної системи захисту інформації) та/або підключення до Інтернету за допомогою захищеного вузла інтернет-доступу (ЗВІД). Підключення до операційного порталу відбувається через тунель, що шифрується за допомогою описаних в державних стандартах протоколів. Також провайдер заявляє про побудову системи управління інформаційної безпеки за стандартом ISO 27001:2013 [8].

Отже, захист інформації в хмарних сховищах пропонується реалізовувати на принципах шифрування даних, впровадження політики доступу на основі електронного цифрового підпису, аналізу підозрілої активності, фізичного ізолювання сегмента хмари згідно з вимогами КСЗІ з використанням сервісів ЗВІД. Хоча деякі реалізації хмарних сховищ і відповідають вимогам КСЗІ, але гарантія надійності збереження даних відсутня через неможливість комплексного контролю користувачів, апаратного та програмного забезпечення за допомогою якого здійснюється робота з хмарними сховищами та віддаленого розміщення серверного обладнання (дуже часто за кордоном). Стандарт ISO 27001:2013, що використовувався деякими провайдерами для побудови системи управління інформаційною безпекою висвітлює загальні положення зі забезпечення інформаційної безпеки, але комплексно не враховує особливості хмарних обчислень й методи забезпечення захисту інформації в сфері хмарних технологій.

Тому доцільно проаналізувати існуючи нормативно-правові документи в сфері захисту інформації в хмарних сховищах, які б враховували особливості побудови та експлуатації цих сховищ.

Метою статті є аналізування проблематики захисту інформаційних ресурсів при використанні хмарних технологій. Для досягнення сформованої мети проаналізовано технології хмарних обчислень та виконано порівняльний аналіз нормативно-правових документів щодо захисту інформації при використанні хмарних технологій.

Викладення основного матеріалу. Спочатку надамо визначення хмарних обчислень, їх призначення та основні характеристики. Під хмарними обчисленнями розуміється результат розвитку багатьох різних технологій, які в комбінації змінили організаційний підхід до побудови інформаційної інфраструктури організації. Хмарні обчислення (cloud computing) – модель надання можливості повсюдного і зручного мережевого доступу на вимогу до пулу налаштованих обчислювальних ресурсів, які підлягають конфігурації (наприклад, мережі, сервери, засоби зберігання, застосунки і сервіси), що можуть оперативно надаватися і звільнятися при мінімальному зусиллі управління або взаємодії з провайдером (постачальником) [3, 9].

Основними характеристиками хмарних обчислень, які відрізняють їх від інших типів обчислень є: самообслуговування на вимогу, об'єднання ресурсів, миттєва еластичність ресурсів, вимірюваний сервіс. Розглянемо кожну з характеристик окремо [3, 9].

1. Самообслуговування на вимогу. Споживач зам необхідності автоматично, без взаємодії з кожним постачальником послуг, може самостійно визначати і змінювати обчислювальні потужності, як-от серверний час, обсяг сховища даних; широкий (універсальний) мережевий доступ. Обчислювальні можливості доступні на великій відстані мережою через стандартні механізми, що сприяє широкому використанню різнорідних платформ клієнта (термінальних пристроїв).
2. Об'єднання ресурсів. Конфігуровані обчислювальні ресурси постачальника об'єднані в єдиний пул для спільного використання розподілених ресурсів великою кількістю споживачів.
3. Миттєва еластичність ресурсів (миттєва масштабованість). Хмарні послуги можуть швидко надаватися, розширюватися, стискатися і звільнятися, виходячи з потреб споживача.
4. Вимірюваний сервіс (облік споживаного сервісу і можливість оплати послуг, які були реально використані). Хмарні системи автоматично керують і оптимізують використання ресурсів завдяки здійснення вимірювань на деякому рівні, що відповідає типу сервісу.

Проаналізувавши загальне визначення хмарних обчислень та їх основні характеристики можна сформулювати основні переваги й недоліки під час роботи з ними. [3, 9]. Хмарні обчислення мають ряд важливих переваг: вся інформація доступна з будь-якого пристрою, (комп'ютер, планшет, смартфон, тощо) підключеного до інтернету. Користувач не прив'язаний до певного робочого місця; скорочення витрат на придбання дорогих потужних комп'ютерів, серверів, немає потреби оплачувати роботу IT-фахівця для обслуговування локального дата-центру; необхідні інструменти для роботи надаються автоматично веб сервісом; високий рівень технологічності обчислювальних потужностей, який надається користувачу, дозволяє зберігати, аналізувати і обробляти дані; оплата сервісів відбувається тільки за необхідності їх використання, при цьому оплата відбувається тільки за необхідний пакет послуг; сучасні хмарні обчислення можуть забезпечувати найвищу надійність, до того ж лише невелика кількість організацій можуть дозволити собі утримувати повноцінний дата-центр; висока відмовостійкість.

Недоліки хмарних обчислень: для роботи з "хмарою" потрібне постійне підключення до Інтернету; користувач не завжди може налаштувати програмне забезпечення, яке використовується за індивідуальними потребами; створення власної "хмари" потребує значних коштів; "хмара" – сховище даних, до яких, використовуючи вразливості системи, можуть отримати доступ зловмисники [9].

Визначивши важливі переваги та основні недоліки хмарних обчислень перейдемо до класифікації та аналізу організацій та органів, які розробляють нормативно-правові документи для хмарних обчислень. Вони створюють міжнародні стандарти і мають наступну ієрархію рівнів:

1. Міжнародний (ISO/IEC [3]);
2. Міждержавний (форуми і консорціуми (Cisco, CSA));
3. Регіональний (європейські органи ETSI, CEN / CENELEC);
4. Національний (закони та державні стандарти, відомчі нормативні документи, керівництва, інструкції, наприклад: (NIST) [10-12].

При стандартизації хмарних технологій кордони держав втрачають обмежувальну роль, так як учасники процесу надання послуг часто знаходяться в різних країнах і на різних континентах. У силу актуалізації забезпечення інформаційної безпеки та відсутності міжнародних стандартів зі сертифікації елементів хмарної інфраструктури, такі елементи (дата-центри, канали і мережі комунікацій) використовують сертифікати безпеки стандартів суміжних напрямів (як міжнародних, так і інших країн).

У сфері управління конфігурацією хмарних технологій багато організацій прагнуть розробляти специфікації для стандартного інтерфейсу прикладного програмування (API), тобто інтерфейсу через який користувачі та оператори керують хмарними обчисленнями та сховищами. Робоча група Відкритого інтерфейсу хмарних обчислень (Open Cloud Computing Interface Working Group – OCCI-WG) організації Open Grid Forum (OGF) визначила та випустила API для управління інфраструктурою як сервісом (IaaS). Інкубатор Open Cloud Standards Incubator (OCSI) робочої групи розподіленого управління (DMTF) також визначив API керування IaaS. А асоціація виробників мереж зберігання даних (SNIA) сформулювала специфікації Cloud Data Management Interface (CDMI – Управління інтерфейсом хмарних даних), яка є API для управління блоками зберігання даних [13].

Організація нестандартних послуг також активно працює в цій галузі. Спільнота з відкритим кодом під назвою “OpenStack”, створена переважно Rackspace і NASA у липні 2010 року, зробила вихідний код програмного забезпечення для керування IaaS відкритим.

Стандартизація хмарних обчислень розпочата промисловими організаціями, які розробляють так звані “стандартні стандарти”. Починаючи з кінця 2009 року, почали діяти органи стандартизації, такі як MCE-T та ISO/IEC JTC1, а також стандартні органи, орієнтовані на інформаційно-телекомунікаційні технології, як-от Інститут інженерів електротехніки та електроніки (IEEE) та Інтернет-технічна робоча група (IETF). У США та Європі стандартизація хмарних обчислень також обговорюються урядовими організаціями.

Існує дві групи органів стандартів форуму, пов’язані з хмарними обчисленнями. Ті, що входять до складу першої групи, включаючи DMTF, OGF і SNIA, активно працюють у сфері мереж та керування розподіленим процесом, а останнім часом додають хмарні обчислення до своїх завдань. Органи другої групи, включаючи OCC, CSA та GICTF, нещодавно засновані для роботи з хмарними обчисленнями.

DMTF (Distributed Management Task Force – Робоча група розподіленого управління). DMTF визначила Open Virtualization Format (OVF), який є стандартним форматом зображення віртуальної машини. Вона започаткувала OCSI у квітні 2009 року та вивчає стандарти, які дозволять взаємодіяти між хмарними системами. CMWG (The Cloud Management Working Group – Робоча група управління хмарами), в якій VMware, Fujitsu та Oracle пропонують відповідний API, створена у червні 2010 року. DMTF у листопаді 2009 року випустила “Білий документ” про сумісність між хмарними системами, а інший – щодо випадків використання управління хмарами та взаємодії в червні 2010 року. Членами Правління є VMware, Microsoft, IBM, Citrix, Cisco та Hitachi.

OGF (Open Grid Forum – Відкритий Грід форум). OGF створив робочу групу OCCI-WG у квітні 2009 року та визначив і випустив специфікацію API [11], що дозволяє керувати комп'ютером та робочими навантаженнями через IaaS. Відкритий інтерфейс хмарних обчислень реалізується у Європі у проекті OpenNebula. Основними учасниками цього проекту є Fujitsu, EMC та Oracle.

SNIA (Storage Networking Industry Association – Асоціація виробників мереж зберігання даних). У квітні 2009 року SNIA заснувала Технічну робочу групу хмарних сховищ (Cloud

Storage Technical Working Group) і випустила CDMI, яка є специфікацією інтерфейсу для керування даними у хмарі. У жовтні 2009 року Асоціація створила підгрупу під назвою CSI (Cloud Storage Initiative – Ініціатива хмарних сховищ) для навчання користувачів та просування ринку хмарних сховищ за допомогою проекту Cloud BUR SIG (Cloud Backup and Recovery Special Interest Group – Група спеціальних інтересів по хмарному резервуванню та відновленню). Членами SNIA є EMC, IBM, Fujitsu та Hitachi.

OCC (Open Cloud Consortium – Відкритий хмарний консорціум). OCC - це некомерційна організація, що утворена в січні 2009 року під керівництвом університету штату Іллінойс у Чикаго. Він спрямований на розробку еталонних тестів за допомогою хмарного випробувального стенду та досягнення сумісності між хмарними системами.

CSA (Cloud Security Alliance – Альянс хмарної безпеки). CSA – це некомерційна організація, створена в березні 2009 року для вивчення найкращих практик забезпечення безпеки хмари та сприяння їх використанню. У квітні 2009 року було опубліковано вказівки щодо забезпечення безпеки хмар.

GICTF (Global Inter-Cloud Technology Forum – Глобальний форум з хмарних технологій). GICTF - це японська організація, що займається вивченням стандартних інтерфейсів між хмарами з метою підвищення надійності хмар. В його склад входять понад 80 корпоративних членів і організацій з промисловості, уряду і наукових кіл. У червні 2010 року вона випустила офіційний документ щодо випадків використання міжхмарного об'єднання і функціональних вимог.

Державні органи в США та Європі також активно працюють у сфері стандартизації, пов’язаної з хмарами. Зокрема NIST та ENISA.

NIST (National Institute of Standards and Technology – Національний інститут стандартів та технологій) – це технічний відділ, який належить Торгово-промисловому департаменту США. Одним з перших документів, який розроблений NIST й який встановлює визначення зі сфери хмарних технологій є “The NIST Definition of Cloud Computing”. В той же час NIST здійснює стандартизацію хмарних технологій за п’ятьма робочими групами. Одна з них – SAJACC (Standards Acceleration to Jumpstart Adoption of Cloud Computing – Прискорення стандартів для швидкого впровадження хмарних обчислень), яка покликана сприяти розробці стандартів хмарних технологій на основі фактичних прикладів та випадків використання.

ENISA (European Union Agency for Network and Information Security – Європейська агенція мереж та інформаційної безпеки). ENISA розробило наступні документи: “Cloud Computing: Benefits, Risks and Recommendations for Information Security”, який надає рекомендації з організації безпеки інформації при хмарних обчисленнях, а також “Cloud Computing Information Assurance Framework”, яка є основою для забезпечення безпеки інформації при хмарних обчисленнях.

Хоч багато організацій обговорюють питання стандартизації хмарних технологій, діяльність щодо консолідації обговорень і рішень нині є недостатньою. Такі заходи проводяться лише частково. Головним питанням є, наскільки добре національні та міжнародні органи стандартизації, які почали повномасштабні дослідження хмарних технологій, можуть співпрацювати з робочими групами розвитку та підтримки хмарних технологій утвореними бізнесом, як новітні світові розробки впровадити до інформаційного простору нашої держави та закріпити в нормативних документах України. Розглянемо деякі основні стандарти забезпечення безпеки інформації в хмарних технологіях.

В даний час два технічних підкомітети Об’єднаного технічного комітету 1 ISO (JTC 1) “Інформаційні технології” ведуть розробку міжнародних стандартів в області хмарних технологій. Ними були розроблені такі документи:

Стандарт ISO/IEC 17788 “Information technology. Distributed application platforms and services. Cloudcomputing. Overview and vocabulary” (“Інформаційні технології. Розподілені прикладні платформи і сервіси. Хмарні обчислення. Загальні положення та словник”).

Стандарт описує концепцію хмарних обчислень і містить ряд термінів і визначень. Він став термінологічної основою для подальшої роботи зі стандартизації в сфері хмарних обчислень. Офіційна публікація стандарту відбулась в 2014 році. [9]

Стандарт ISO/IEC 17789 "Information technology. Cloud computing. Reference architecture" ("Інформаційні технології. Хмарні обчислення. Еталонна архітектура"). Стандарт містить огляд загальних понять і характеристик хмарних обчислень, типів хмар, компонентів хмарних обчислень сторін-учасниць. У ньому зроблено наголос на вимоги до того, що повинні забезпечувати хмарні сервіси, а не на питаннях проектування і впровадження відповідних рішень. [3]

Технічна специфікація ISO/IEC TS 27017 "Information technology - Security techniques - Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002" ("Інформаційні технології. Методи захисту. Звід практик стосовно заходів інформаційної безпеки, що ґрунтуються на ISO/IEC 27002, для хмарних послуг") [14]. Стандарт містить рекомендації щодо забезпечення інформаційної безпеки хмарних обчислень. Він спирається на переглянуту версію ISO/IEC 27002 і містить здебільшого рекомендації з реалізації описаних в цьому документі заходів інформаційної безпеки в контексті хмарних обчислень.

Стандарт ISO/IEC 27018 "Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors" ("Інформаційні технології. Методи захисту. Кодекс усталеної практики для захисту персональної ідентифікаційної інформації (PII) у загальнодоступних хмарах, що діють як процесори PII") [15]. Стандарт призначений для постачальників послуг "публічної хмари", які ведуть обробку персональних даних (і є операторами персональних даних). Він містить рекомендації щодо різних аспектів і елементів захисту персональних даних і недоторканності особистої інформації в публічній хмарі. Стандарт не дублює або модифікує рекомендації стандарту ISO/IEC 27002. У ньому визначені додаткові цілі і заходи контролю і управління, пов'язані із захистом персональних даних в хмарному середовищі.

З прийняттям у 2014 році міжнародного стандарту ISO 17788 [9] регламентовано 7 репрезентативних категорій хмарних послуг: CaaS (Communications as a Service – Зв'язок як послуга), CompaaS (Compute as a Service – Обчислення як послуга), DSaaS (Data Storage as a Service – Зберігання даних як послуга), IaaS (Infrastructure as a Service – Інфраструктура як послуга), NaaS (Network as a Service – Мережа як послуга), PaaS (Platform as a Service – Платформа як послуга), SaaS (Software as a Service – Програмне забезпечення як послуга). А також додаткові категорії хмарних послуг: Database as a Service (База даних як послуга), Desktop as a Service (Робочий стіл як послуга), Email as a Service (Електрона пошта як послуга), Identity as a Service (Ідентифікація як послуга), Management as a Service (Управління як послуга), Security as a Service (Безпека як послуга). Надамо пояснення основних типів послуг в сфері хмарних обчислень:

Програмне забезпечення як послуга. У цій моделі надання хмарних обчислень споживач використовує застосунки постачальника, що запущені в хмарній інфраструктурі та які доступні клієнту через веб браузер або інтерфейс програми. Споживачі не можуть керувати і контролювати те, що лежить в основі інфраструктури хмари, включаючи мережу, сервери, операційні системи, сховища даних або навіть змінювати параметри налаштування конкретного застосунку.

Платформа як послуга. Модель надання хмарних обчислень, при якій споживач отримує доступ до використання програмної платформи: операційних систем, систем управління базами даних, прикладного програмного забезпечення, засобів розробки і тестування програмного забезпечення. Фактично споживач отримує в оренду комп'ютерну платформу зі встановленою операційною системою і спеціалізованими засобами для розробки, розміщення і управління веб застосунками. Споживач не управляє основною інфраструктурою хмари, включаючи мережу, сервери, операційні системи або сховища

даних, але управляє розгорнутими застосунками і можливо параметрами налаштування конфігурації середовища оточення.

Інфраструктура як послуга. Модель надання хмарних обчислень, при якій споживач отримує можливість управляти засобами обробки і зберігання, а також і іншими фундаментальними обчислювальними ресурсами (віртуальними серверами і мережевою інфраструктурою), на яких він може самостійно встановлювати операційні системи та прикладні програми за власною потребою. Тобто споживач орендує абстрактні обчислювальні потужності (серверний час, дисковий простір і пропускну здатність мережевих каналів) або використовує послуги аутсорсингу інфраструктури. Споживач не управляє основною інфраструктурою хмари, але управляє операційними системами, сховищем і розгорнутими ним застосунками.

Виходячи з вищевикладеного визначення хмарних обчислень, хмарні сервіси можна представити у вигляді багатошарової моделі, що складається з трьох основних шарів: IaaS, PaaS, SaaS. Базисом або фундаментом хмарних сервісів є фізична інфраструктура (physical infrastructure), тобто сервери, сховища, мережі та системне програмне забезпечення хмарного дата-центру або мережі взаємопов'язаних хмарних дата-центрів.

У проекті стандарту [16], крім перерахованих, представлені також послуги: HaaS (Hardware as a service – Апаратне забезпечення як послуга), BPaaS (Business process as a service – Бізнес-процес як послуга), DaaS (Data as a service – Дані як послуга), TaaS (Trust as a service – Довіра як послуга), SDPaaS (Service delivery platform as a service – Хмарне середовище розробки як послуга), TraaaS (Transparency as a service – Прозорість як послуга), WaaS (Workplace as a service – Робоче місце як послуга). Міжнародний стандарт ISO 17788 також не обмежує список нових хмарних послуг, так що в майбутньому варто очікувати розширення списку послуг і узгодження їх назв і позначень.

Приклад стандартної архітектури системи хмарних обчислень описано в стандарті Національного Інституту стандартів і технологій США (National Institute of Standards and Technology, NIST) NIST SP 500-299 [11]. Мета цього стандарту полягає у визначені орієнтованої на безпеку формальної архітектурної моделі хмарних обчислень, а також ідентифікації основних наборів компонентів безпеки, які можна реалізувати в хмарній екосистемі для захисту середовища, операцій та даних.

В свою чергу розроблене CSA Керівництво з безпеки для критично важливих областей хмарних обчислень (Security Guidance for Critical Areas of Focus in Cloud Computing) надає детальні рекомендації щодо зниження ризику при впроваджені хмарних обчислень, а також які комбінації розгортання й моделей обслуговування в хмарних обчисленнях є прийнятними [17].

Провівши аналіз нормативно-правових документів в сфері хмарних обчислень було визначено множину моделей послуг хмарних обчислень. На основі цього аналізу наведемо відображеність моделей послуг у нормативно-правових документах (табл. 1).

Таблиця 1 – Відображеність моделей послуг у нормативно-правових документах

Моделі послуг	NIST	ГОСТ	ISO	CSA
IaaS	+	+	+	+
PaaS	+	+	+	+
SaaS	+	+	+	+
NaaS		+	+	
WaaS/DaaS		+/–	–/+	
CaaS		+	+	
Haas/CompaaS		+/–	–/+	
SecaaS		+	+	
BPaaS		+		

Продовження таблиці 1

DaaS/DSaaS		+/–	–/+	
TaaS		+		
SDPaaS		+		
TraaaS		+		
Database as a Service			+	
Email as a Service			+	
Identify as a Service			+	
Management as a Service			+	

Як висновок, можна стверджувати, що найбільш повно моделі послуг представлені в нормативних документах щодо хмарних обчислень ГОСТ та ISO.

Також під час аналізу нормативно-правових документів в сфері хмарних обчислень були виокремленні суб’єкти взаємодії (табл. 2) й визначено, що таким суб'єктам, як Cloud Auditor, Cloud Broker і Cloud Partner в кожному нормативному документі делегуються частково різні обов’язки, які описують функції посередника між Cloud Consumer і Cloud Provider. В свою чергу Cloud Consumer і Cloud Provider мають схожі ролі в моделі взаємодії в сфері хмарних обчислень в усіх представлених нормативних документах .

Таблиця 2 – Суб'єкти взаємодії в сфері хмарних обчислень

Суб`єкти	NIST	ГОСТ	ISO	CSA
Cloud Consumer	+	+	+	+
Cloud Provider	+	+	+	+
Cloud Auditor	+			+
Cloud Broker	+			
Cloud Partner			+	

Ще одним напрямком аналізу зазначених стандартів було виділення та інтеграція методів захисту інформації в сфері хмарних обчислень. На основі цього можна зробити висновок, що найбільш цим методам відповідають стандарти ISO та проект ГОСТ. Тобто для подальшого удосконалення та розвитку вітчизняної нормативно-правової бази у сфері захисту інформації в хмарних обчисленнях можна брати за основу стандарти ISO та проект ГОСТ, з врахуванням особливостей зазначених у інших стандартах.

Таблиця 3 – Методи захисту інформації в сфері хмарних обчислень

Методи	NIST	ISO	ГОСТ	CSA
Криптографічні методи		+	+	
Управління кіберінцидентами	+	+	+	
Управління ідентифікацією	+	+	+	+
Системи управління інформаційною безпекою	+	+	+	
Оцінка інформаційної безпеки IT-систем		+		+

Продовження таблиці 3

Мережева інформаційна безпека		+		+
Автоматизований і неперервний моніторинг інформаційної безпеки		+	+	
Гарантований супровід програмного забезпечення		+	+	+
Управління ризиками	+	+		+
Система інженерії інформаційної безпеки		+		

Висновок. Одним з напрямом вирішення завдання створення захищених дата-центрів є їх створення на основі використання хмарних технологій. Прогалини вітчизняної нормативно-правової бази у сфері захисту інформації в хмарних обчисленнях вимагають перегляду й аналізу національних й міжнародних інституцій й об'єднань, які займаються проблематикою стандартизації й розвитку хмарних технологій. Проведений аналіз показав множину органів стандартизації й їх вплив на розвиток хмарних технологій взагалі, й на проблематику захисту хмарних обчислень зокрема. Наведені стандарти різняться щодо повноти опису моделі послуг хмарних обчислень, хоча можна виділити три основні моделі послуг (IaaS, PaaS, SaaS) які зазначені в кожному стандарті. Також наведені в стандартах суб'єкти взаємодії в сфері хмарних обчислень мають різні обов'язки посередництва між двома схожими за функціями в різних стандартах суб'єктами (Cloud Consumer і Cloud Provider). Методи ж захисту інформації в сфері хмарних обчислень найбільш повно описані в ISO 17788 та проекті ГОСТ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Президент України (2017, Лют. 13). *Указ Президента України № 32/2017, Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року "Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації"*. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/32/2017. Дата звернення: Серп. 25, 2019.

[2] ДСТСЗІ СБ України. (2005, Лист. 8). *НД ТЗІ 3.7-003, Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.* [Електронний ресурс]. Доступно: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835. Дата звернення: Серп. 25, 2019.

[3] International Organization for Standardization. (2014, Okt. 15). ISO/IEC 17789, Information technology. Cloud computing. Reference architecture [Online]. Available: https://www.iso.org/standard/60545.html. Accessed on: Aug. 25, 2019.

[4] І.Ф. Абулов, та І.Д. Горбенко, "Хмарні обчислення та аналіз питань інформаційної безпеки в хмарі", *Прикладная радиоэлектроника*, т. 12, № 2. с. 194-201, 2013.

[5] Т.Г. Білова, та В.О. Ярута, "Проблеми шифрування даних в хмарних обчисленнях", *Системи обробки інформації*, вип. 10, с. 79-81, 2015.

[6] У. Шнайдер, "Безопасность при использовании облачных сервисов", *Журнал сетевых решений/LAN*, № 04. [Электронный ресурс]. Доступно: http://www.osp.ru/lan. Дата обращения: Авг. 08, 2019.

[7] Хмарні платформи De Novo. [Електронний ресурс]. Доступно: https://www.de-novo.biz/about. Дата звернення: Серп. 25, 2019.

[8] International Organization for Standardization. (2013, Okt. 1). *ISO/IEC 27001, Information technology. Information security management systems. Requirements*. [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Aug. 25, 2019.

[9] International Organization for Standardization. (2014, Okt. 10). *ISO/IEC 17788, Information technology. Cloud computing. Overview and vocabulary*. [Online]. Available https://www.iso.org/standard/60544.html. Accessed on: Aug. 25, 2019.

[10] National Institute of Standards and Technology. (2011, Sept. 28). *NIST Special Publication 800-145, The NIST Definition of Cloud Computing.* [Online]. Available https://csrc.nist.gov/publications/detail/sp/800-145/final. Accessed on: 25.08.2019. DOI: 10.6028/NIST.SP.800-145.
[11] National Institute of Standards and Technology. (2013, May 24). NIST Special Publication 500-299 (Draft), NIST Cloud Computing Security Reference Architecture. Working Document. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/500-299/draft. Accessed on: Aug. 25, 2019.
[12] National Institute of Standards and Technology. (2011, Aug. 10). *NIST Special Publication 500-291, NIST Cloud Computing Standards Roadmap.* [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909024. Accessed on: 25.08.2019.
[13] Cloud Data Management Interface. SNIA. [Online]. Available: https://www.snia.org/sites/default/files/CDMI_Spec_v1.1.1.pdf. Accessed on: Aug. 25, 2019.
[14] International Organization for Standardization. (2015, Dec. 8). *ISO/IEC TS 27017, Information technology. Security techniques. Information security management. Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002.* [Online]. Available: https://www.iso.org/standard/43757.html. Accessed on: Accessed on: Aug. 25, 2019.
[15] International Organization for Standardization. (2019, Jan. 24). ISO/IEC 27018, Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. [Online]. Available: https://www.iso.org/standard/76559.html. Accessed on: Aug. 25, 2019.
[16] Федеральное агентство по техническому регулированию и метрологи. *Проект ГОСТ Р, Защита информации. Требования по защите информации, обрабатываемой с использованием технологий "Облачных вычислений". Основные положения*. [Электронный ресурс]. Режим доступа: http://docs.cntd.ru/document/1200102839. Дата обращения: Авг. 25, 2019.
[17] Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf. Accessed on: Aug. 25, 2019.

Стаття надійшла до редакції 08.09.2019.

REFERENCE

[1] President of Ukraine. (2017, Febr. 13). *Decree of the President of Ukraine № 32/2017, On the decision of the National Security and Defense Council of December 29, 2016 "On cyber security threats to the state and urgent measures to neutralize them"*. [Online]. Available: https://zakon.rada.gov.ua/laws/show/32/2017. Accessed on: Aug. 25, 2019.
[2] DSTSIP SS of Ukraine. (2005, Nov. 8). *ND TZI 3.7-003, The order of carrying out works on creation of the complex system of information protection in the information and telecommunication system.* [Online]. Available: http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835. Accessed on: Aug. 25, 2019.
[3] International Organization for Standardization. (2014, Okt. 15). *ISO/IEC 17789, Information technology. Cloud computing. Reference architecture* [Online]. Available: https://www.iso.org/standard/60545.html. Accessed on: Aug. 25, 2019.
[4] I.F. Abulov, and I.D. Gorbenko, "Cloud computing and analysis of information security issues in the cloud", *Applied Radio Electronics*, vol. 12, no. 2, pp. 194-201, 2013.
[5] T.G. Bilova, and V.O. Yarutova, "Data encryption problems in cloud computing. Information processing systems", no. 10, pp. 79-81, 2015.
[6] U. Shnaider, "Cloud computing and analysis of information security issues in the cloud". *Applied Radio Electronics/LAN*, no. 4. [Online]. Available: http://www.osp.ru/lan. Accessed on: Aug. 25, 2019.
[7] Cloud platforms De Novo. [Online]. Available: https://www.de-novo.biz/about. Accessed on: Aug. 25, 2019.

[8] International Organization for Standardization. (2013, Okt. 1). *ISO/IEC 27001, Information technology. Information security management systems. Requirements.* [Online]. Available: https://www.iso.org/standard/54534.html. Accessed on: Aug. 25, 2019.
[9] International Organization for Standardization. (2014, Okt. 10). *ISO/IEC 17788, Information technology. Cloud computing. Overview and vocabulary.* [Online]. Available https://www.iso.org/standard/60544.html. Accessed on: Aug. 25, 2019.
[10] National Institute of Standards and Technology. (2011, Sept. 28). *NIST Special Publication 800-145, NIST Definition of Cloud Computing.* [Online]. Available https://csrc.nist.gov/publications/detail/sp/800-145/final. Accessed on: 25.08.2019. DOI: 10.6028/NIST.SP.800-145.
[11] National Institute of Standards and Technology. (2013, May 24). NIST Special Publication 500-299 (Draft), NIST Cloud Computing Security Reference Architecture. Working Document. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/500-299/draft. Accessed on: Aug. 25, 2019.
[12] National Institute of Standards and Technology. (2011, Aug. 10). *NIST Special Publication 500-291, NIST Cloud Computing Standards Roadmap.* [Online]. Available: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=909024. Accessed on: 25.08.2019.
[13] Cloud Data Management Interface. SNIA. [Online]. Available: https://www.snia.org/sites/default/files/CDMI_Spec_v1.1.1.pdf. Accessed on: Aug. 25, 2019.
[14] International Organization for Standardization. (2015, Dec. 8). *ISO/IEC TS 27017, Information technology. Security techniques. Information security management. Guidelines on information security controls for the use of cloud computing services based on ISO / IEC 27002.* [Online]. Available: https://www.iso.org/standard/43757.html. Accessed on: Aug. 25, 2019.
[15] International Organization for Standardization. (2019, Jan. 24). ISO/IEC 27018, Information technology. Security techniques. Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. [Online]. Available: https://www.iso.org/standard/76559.html. Accessed on: Aug. 25, 2019.
[16] Federal Agency on Technical Regulating and Metrology. *GOST R, Project Information protection. Requirements for the protection of information processed using "Cloud computing" technologies. Basic provisions.* [Online]. Available: http://docs.cntd.ru/document/1200102839. Accessed on: Aug. 25, 2019.
[17] Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0. [Online]. Available: https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf. Accessed on: Aug. 25, 2019.

ARTEM ZHYLIN,
ANDRII DIVITSKYI,
ANNA KOZACHOK

PROBLEMS OF PROTECTION OF INFORMATIONAL RESOURCES WHEN USING CLOUD TECHNOLOGIES

The solution to the problem of secure data centers for storage of information and state electronic information resources is offered through the implementation of cloud technologies. State regulatory acts don`t solve the problem of providing security status during the remote processing of information in data centers using cloud technologies, so the experience of international standards and best practices in this field are analyzed. The purpose of the article is to analyze the problem of information resources protection when using cloud technologies. To achieve this goal, cloud computing technologies are analyzed and comparative analysis of regulatory documents on information security when using cloud technologies is conducted. Unique definitions and characteristics of cloud computing which differentiate them from other types of computing technologies are also described, including such terms as on-demand self-service, resource pooling,

instant resilience of resources, measured service. The classification and analysis of organizations and authorities that develop regulatory documents in the sphere of cloud computing is provided and described. These establishments work on making international standards and have the following hierarchy of levels: international (ISO / IEC), interstate (forums and consortia (Cisco, CSA)), regional (European ETSI, CEN / CENELEC), national (laws and national standards, departmental regulations) , guides, instructions, for example: (NIST). The great consortia's role in standardizing and developing both cloud technologies and information protection issues when using them is highlighted. The description of these consortia and their activity vectors are outlined. The documents, created by them, in the field of cloud security are reviewed and compared to ISO 17788, NIST SP 500-299, Security Guidelines for Critical Cloud Computing CSAs and GOST R "Information Protection. Requirements for the protection of information, processed with using the technology of "cloud computing". Basic provisions". Basing on the conducted analysis, the reflection of service models in the regulatory documents is presented and the information on the methods of data protection in the field of cloud computing, which is available in the documents, is summarized.

Keywords: cloud technologies, cloud repositories, information security, service models, standards, methods of information security/

Жилін Артем Вікторович, кандидат технічних наук, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ.

ORCID: 0000-0002-4959-612X.

E-mail: zhylinartem@gmail.com.

Дівіцький Андрій Сергійович, старший викладач кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ.

ORCID: 0000-0002-9261-9841.

E-mail: 70div@ukr.net.

Козачок Анна Олександрівна методист першої категорії навчального відділу, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ.

ORCID: 0000-0001-8898-1429.

E-mail: kozachok2010@ukr.net.

Zhylin Artem, candidate of technical sciences, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Divitskyi Andrii, senior lecturer at the public information resources security academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Kozachok Anna, methodist of the first category of the educational department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.