УДК 004.75:004.05

ХМАРНІ ОБЧИСЛЕННЯ ТА АНАЛІЗ ПИТАНЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРІ

І.Ф. АУЛОВ, І.Д. ГОРБЕНКО

Розглядається сучасний стан застосування та розвитку хмарних обчислень, основні переваги та недоліки їх використання у державах, на підприємствах та в науковій діяльності. Визначаються та аналізуються стандарти, нормативні та керівні документи в галузі інформаційної безпеки хмарних обчислень, що розроблені Cloud Security Alliance (CSA), Європейським агентством мережної та інформаційної безпеки (ENISA) і Національним інститутом стандартів і технологій (NIST), а також наводяться результати детального аналізу питань інформаційної безпеки в хмарі.

Ключові слова: хмарні обчислення, інформаційна безпека, порівняльний аналіз, недоліки та переваги обчислень в хмарах.

ВСТУП

В останні роки ефективного застосування набувають хмарні технології або хмарні обчислення (англ. Cloud computing).

В [1] дається визначення хмарних обчислень як моделі забезпечення повсюдного та зручного доступу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними затратами або зверненням до провайдера.

До хмарних технологій проявляють зацікавленість як великі компанії, які намагаються оптимізувати свої витрати на IT-інфраструктуру підприємства, так і малі компанії, які не мають можливості відразу розгорнути свою власну інфраструктуру. Також зацікавлені звичайні користувачі, що можуть отримати такі послуги як зберігання даних, використання програм тощо. Зростання інтересу до технології хмарних обчислень пов'язано з економічним ефектом від їх використання. В ході їх використання споживачі можуть істотно знизити капітальні витрати на побудову центрів обробки даних, закупівлю серверного та мережного обладнання, апаратних і програмних рішень, забезпечення безперервності і працездатності, а також час побудови та введення в експлуатацію великих об'єктів інфраструктури інформаційних технологій. Всі ці проблемні питання за даних умов перекладаються з користувачів на провайдерів хмарних послуг, а користувач лише оплачує фактично надані послуги. Також хмарні сервіси надають їх користувачам гнучкість у налаштуванні таких параметрів, як обчислювальна потужність, обсяг файлового сховища, склад програмного забезпечення тощо. Однак, незважаючи на явні переваги, під час використання хмарних обчислень необхідно вирішувати і ряд проблемних питань. Основними з них є довіра до постачальника сервісу, забезпечення конфіденційності, цілісності, справжності та неспростовності інформації на усіх етапах її існування, безперебійність в роботі, захист від несанкціонованого доступу (НСД) та збереження особистих даних користувачів, які передаються та обробляються в хмарі. Метою цієї статті є класифікація та огляд основних технологій хмарних обчислень, а також аналіз сучасного стану застосування та досліджень в галузі безпеки хмарних технологій.

1. ОСНОВНІ ПОНЯТТЯ ТА ВИЗНАЧЕННЯ

NIST США запропонував модель хмари, яка складається з п'яти основних характеристик, трьох моделей обслуговування і чотирьох моделей розгортання [1].

Основними характеристиками хмари є такі:

– Якість самообслуговування на вимогу (*англ.* on-demand self-service), коли споживач не взаємодіючи безпосередньо з представником постачальника послуг, може самостійно визначати та змінювати такі обчислювальні потреби як серверний час, швидкість доступу та обробки даних, обсяг збережених даних тощо.

– Універсальність доступу з використанням мережі (*англ.* broad network access), коли послуги доступні споживачам через мережі передачі інформації, незалежно від термінального пристрою клієнтських платформ (наприклад, мобільні телефони, планшети, ноутбуки та робочі станції).

– Ступінь об'єднання ресурсів (*англ.* resource pooling), коли постачальник послуг об'єднує ресурси для обслуговування декількох споживачів, використовуючи багатокористувальницьку модель з різними фізичними і віртуальними ресурсами, які динамічно розподіляються та перерозподіляються між користувачами відповідно до попиту. При цьому клієнт не має змоги контролювати розташування ресурсу або не знає точне місце його розташування, але в змозі вказати місце розташування на більш високому рівні абстракції (наприклад, країну, штат або центр обробки даних). Як такі ресурси можуть виступати: сховища даних, обчислювальні потужності, пам'ять та пропускна здатність мережі.

– Достатня еластичність (*англ.* rapid elasticity), коли послуги в будь-який момент часу без додаткових витрат на взаємодію з постачальником можуть бути надані, розширені, звужені, як правило, в автоматичному режимі. Для споживача

такі можливості провайдера з надання послуг здаються необмеженими та можуть бути надані в будь-якій кількості і в будь-який час.

– Облік споживання (*англ.* measured service), коли сервіс хмари автоматично управляє та оптимізує використання ресурсів користувачами за рахунок вимірювань на деякому рівні абстракції (наприклад, обсяг збережених даних, пропускна здатність, кількість користувачів, кількість транзакцій). Контроль над використанням ресурсів, можливість управління ресурсами та формування звіту з споживання забезпечують прозорість як для постачальника, так і для споживача послуг.

В [1] також визначено такі моделі обслуговування за допомогою хмари:

– Програмне забезпечення як послуга (SaaS) – модель, коли споживачу надається можливість використання додатків постачальника, що працюють на хмарній інфраструктурі. Програми є доступними з різних клієнтських пристроїв або через інтерфейс тонкого клієнту, такий як веб-браузер (наприклад, веб-пошта) або інтерфейсу програми. Споживач не контролює та не керує базовою інфраструктурою хмари, в тому числі мережею, серверами, операційною системою, зберіганням, або навіть індивідуальними можливостями додатка, за винятком обмежених користувальницьких параметрів конфігурації додатка. Прикладами такої моделі є сервіси Gmail та Google docs.

– Платформа як послуга (PaaS) – модель, коли споживачу надається можливість розгортання на базі хмарної інфраструктури власних чи придбаних додатків, які створені за допомогою мови програмування, бібліотек, служб та засобів, що підтримуються постачальником. Споживач не контролює та не керує базовою інфраструктурою хмари, в тому числі мережею, серверами, операційною системою, або зберіганням, але має контроль над розгорнутими додатками і, можливо, параметрами конфігурації середовища, в якому працюють додатки. Наприклад, Google Apps надає додатки для бізнесу в режимі онлайн, доступ до яких відбувається за допомогою Інтернет-браузера, тоді як програмне забезпечення та дані зберігаються на серверах Google.

– Інфраструктура як послуга (IaaS) – модель, коли споживачу надається можливість обробки, зберігання, доступ до мережі та інших основних обчислювальних ресурсів, де споживач має можливість розгортання і запуску довільного програмного забезпечення, яке може включати в себе операційні системи та програми. Споживач не контролює та не керує базовою інфраструктурою хмари, але має контроль над операційними системами, зберіганням та розгорнутими додатками, і, можливо, обмежений контроль вибору мережних компонентів (наприклад, мережними екранами). Найбільшими гравцями на ринку інфраструктури як послуги є Amazon, Microsoft, VMWare, Rackspace та Red Hat. Хоча деякі з них пропонують більше, ніж просто інфраструктуру, їх об'єднує мета продавати базові обчислювальні ресурси.

Обчислювальна хмара може бути розгорнута як: приватна, публічна, громадська або гібридна [1].

Приватна хмара (*англ.* private cloud) – це хмарна інфраструктура, яка призначена для використання виключно однією організацією, що включає декількох користувачів (наприклад, підрозділів). Приватна хмара може перебувати у власності, керуванні та експлуатації як самої організації, так і третьої сторони (чи деякої їх комбінація). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника.

Громадська хмара (*англ.* community cloud) – це хмарна інфраструктура, яка призначена для використання конкретною спільнотою споживачів із організацій, що мають спільні цілі (наприклад, місію, вимоги щодо безпеки, політику та відповідність різноманітним вимогам). Громадська хмара може перебувати у спільній власності, керуванні та експлуатації однієї чи більше організацій зі спільноти або третьої сторони (чи деякої їх комбінації). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника.

Публічна хмара (*англ.* public cloud) – це хмарна інфраструктура, яка призначена для вільного використання широким загалом. Публічна хмара може перебувати у власності, керуванні та експлуатації комерційних, академічних (освітніх та наукових) або державних організацій (чи будь-якої їх комбінації). Публічна хмара знаходиться в юрисдикції постачальника хмарних послуг.

Гібридна хмара (*англ.* hybrid cloud) – це хмарна інфраструктура, що складається з двох або більше різних хмарних інфраструктур (приватних, громадських або публічних), які залишаються унікальними сутностями, але з'єднані між собою стандартизованими або приватними технологіями, що дозволяють переносити дані та прикладні програми (наприклад, використання ресурсів публічної хмари для балансування навантаження між хмарами).

2. ОСНОВНІ ПИТАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРІ

На сьогодні провідними організаціями, що займаються питаннями безпеки в хмарі, є Альянс безпека в хмарі (Cloud Security Alliance, CSA), що складається з представників IT-індустрії, а також дві державні організації Європи та США: Європейське агентство мережної та інформаційної безпеки (ENISA) і Національний інститут стандартів і технологій (NIST).

Кожна з організацій створила відповідний документ з класифікацією всіх існуючих проблем інформаційної безпеки(ІБ) в хмарі. Розглянемо їх та проведемо порівняння.

2.1 Таксономія питань ІБ у хмарі CSA

CSA є некомерційною організацією, що створена наприкінці 2008 року організаціями, засновниками якої виступили великі IT-компанії,

зацікавлені у впровадженні хмарних технологій: Google, Microsoft, IBM, Salesforce.com, VMware та інші.

Основним документом, який розглядає проблеми безпеки в хмарі, є «Керівництво з безпеки критичних областей для хмарних обчислень». Перша версія його була опублікована в 2009 році. Нами розглянута остання, 3 версія цього документу, яка доступна на офіційному сайті організації. Основними складовими вимог ІБ у хмарах, що рекомендуються до розгляду та аналізу, є такі [4]:

1 *Організаційні та правові питання ІБ*

1.1 Управління ризиками.

1.1.1 Корпоративне управління ризиками.

1.1.2 Управління ризиками підприємства та постачальника послуг.

1.1.3 Управління інформаційними ризиками

1.2 Правові питання та законодавство.

1.2.1 Стандартизація, міжнародне законодавство, узгодження законодавства держав.

1.2.2 Договір між постачальником та клієнтом.

1.2.3 Право власності на інформацію, що обробляється в хмарі.

1.3 Відповідність вимогам та аудит.

1.3.1 Проведення експертизи; моніторинг, тестування та оновлення програмного та апаратного забезпечення постачальника.

1.3.2 Дотримання існуючих міжнародних та державних законів.

1.3.3 Аудит безпеки постачальника послуг.

1.4 Управління інформацією та безпекою даних.

1.4.1 Безпека даних (запобігання витоку, несанкціонованого доступу, втраті тощо).

1.4.2 Управління життєвим циклом даних (створення, зберігання, використання, обмін, архівування, відновлення, знищення).

1.4.3 Керування розташуванням даних.

1.4.4 Управління авторським правом (DRM).

1.5 Переносимість та інтероперабельність.

1.5.1 Сумісність апаратного, програмного забезпечення, архітектурних рішень постачальників.

1.5.2 Стандартизований інтерфейс взаємодії з постачальником хмарних послуг.

2 Технічні питання ІБ

2.1 Традиційна безпека забезпечення безперервності бізнесу та аварійного відновлення.

2.1.1 Захист від стихійних лих, техногенних катастроф та ін.

2.1.2 Захист від людського фактору та обслуговуючого персоналу.

2.2 Операції центру обробки даних.

2.2.1 Взаємодія між центрами постачальника.

2.2.2 Взаємодія між різними постачальниками.

2.3 Реагування на інциденти, повідомлення про них та відновлення.

2.3.1 Попередження виникнення інцидентів ІБ.

2.3.2 Визначення та аналіз інцидентів ІБ.

2.3.3 Відновлення після інцидентів безпеки.

2.4 Безпеки додатків та програм.

2.4.1 Контроль якості, тестування на відмову, безпечність програмного забезпечення.

2.4.2 Розмежування доступу користувачів до додатків.

2.4.3 Моніторинг активності додатків.

2.4.4 Виявлення небезпечних програм та забезпечення безпеки існуючих.

2.5 Шифрування та управління ключами.

2.5.1 Альтернативні підходи до шифрування даних у хмарі.

2.5.2 Криптографія в хмарі.

2.5.3 Шифрування баз даних.

2.5.4 Управління ключами в хмарі (генерація, використання, зберігання, знищення, відновлення).

2.6 Ідентифікація і управляння доступом.

2.6.1 Моделі ідентифікації в хмарі.

2.6.2 Керування профілями користувачів.

2.6.3 Надання послуг ідентифікації, автентифікації, спільного доступу до інформації в хмарі або ресурсів.

2.6.4 Реалізація ідентифікації користувачів у програмному забезпеченні.

2.6.5 Доступність, цілісність даних, доступ до даних авторизованих користувачів.

2.7 Віртуалізація.

2.7.1 Забезпечення захисту гістьової віртуальної машини від атак.

2.7.2 Механізми захисту від неправомірних дій адміністраторів.

2.7.3 Питання швидкодії, пікового збільшення навантаження, збільшення числа вузлів.

2.7.4 Забезпечення безпеки даних на рівні віртуальної машини.

2.7.5 Забезпечення цілісності образів віртуальних машин.

2.8 Безпека як сервіс.

2.8.1 Продаж послуг безпеки.

2.8.2 Проблеми при реалізації послуги безпеки.

2.8.3 Класифікація послуг безпеки.

Документ окрім питань ІБ розглядає також архітектуру побудови хмари та надає рекомендації та шляхи вирішення цих проблем. У цілому питання ІБ у хмарі поділяються на дві великі групи: питання управління ІБ у хмарі (організаційні питання ІБ) та ІБ у хмарі під час її використання (технічні питання ІБ). Кожна з груп розбита на більш малі, що називаються доменами. Домени, що відносяться до організаційних, у першу чергу розглядаються з метою вироблення рішень правових питань, питань політики ІБ, управління ризиками та стандартизація. В рамках технічних питань розглядаються питання реалізації та впровадження захисту в хмарі.

2.2 Таксономія питань ІБ у хмарі ENISA

Європейське агентство з мережної та інформаційної безпеки (ENISA) є організацією, діяльність якої спрямована на «підвищення здатності Європейського Союзу, держав-членів ЄС та бізнес-спільноти на попередження, ліквідацію

і реагування на проблеми мережної та інформаційної безпеки» [6].

Організацією ENISA було підготовлено і опубліковано документ "Безпека хмарних обчислень та оцінка ризиків" [5], в якому були розглянуті питання інформаційної безпеки в хмарі, їх переваги та недоліки, існуючі ризики, аналіз та шляхи їх зменшення, існуючі загрози в середовищі хмарних обчислень. Згідно з цим документом можна виділити такі ризики ІБ, які існують в хмарі :

1 Організаційні питання ІБ

1.1 Втрата можливості керування користувачем деякими налаштуваннями безпеки в хмарі.

1.2 Замкнутість користувача на одному постачальнику послуг у зв'язку з відсутністю переносимості та інтероперабельності розгорнутої інфраструктури.

1.3 Дотримання вимог стандартів.

1.4 Втрати ділової репутації постачальника.

1.5 Припинення роботи сервісом хмари.

1.6 Відмова в роботі одного з постачальників.

1.7 Придбання провайдера хмарних послуг.

2 Правові питання ІБ

2.1 Судовий розгляд та законодавство в сфері електронних даних.

2.2 Ризик зміни юрисдикції.

2.3 Ризики щодо захисту даних.

2.4 Ризики ліцензування.

2.5 Право власності електронних даних.

3 Технічні питання ІБ

3.1 Порушення ізоляції даних користувачів.

3.2 Часткове або неповне знищення даних користувача.

3.3 Вичерпання ресурсів.

3.4 Загроза інсайдерів в інфраструктурі постачальника послуг.

3.5 Ризики інтерфейсу управління.

3.6 Перехоплення даних зловмисником при передачі.

3.7 Витік даних при завантаженні та скачуванні.

3.8 Розподілена відмова в обслуговуванні (DDoS-атака).

3.9 Економічна відмова в обслуговуванні (EDoS-атака).

3.10 Втрата ключів шифрування.

3.11 Проведення сканування та тестування з метою виявлення вразливостей.

2.3 Таксономія питань ІБ у хмарі NIST

З метою впровадження хмарних обчислень урядом США в організації NIST було замовлено розроблення стандарту з забезпечення безпеки та конфіденційності в громадських хмарах. Тому починаючи з 2011 року NIST опублікував ряд документів, які давали визначення хмарним обчисленням, розглядали питання ІБ у хмарі, пропонували архітектуру безпеки в хмарі, давали рекомендації з оцінки та усунення існуючих ризиків ІБ у хмарі.

Класифікація питання ІБ у хмарі розглядається в таких документах NIST: «Посібник з безпеки та конфіденційності в громадських хмарних обчисленнях» [7] та «Короткий огляд хмарних обчислень та рекомендації» [8]. На відміну від розглянутих таксономій питань ІБ у хмарі CSA та ENISA, в таксономії NIST питання ІБ чітко не поділяють на такі рівні як організаційні питання, правові питання та технічні питання ІБ. Розглянемо їх в натуральному вигляді.

1 Управління

1.1 Контроль і нагляд урядовою організацією за політикою, процедурами та стандартами в ході розробки додатків та інформаційних технологій, одержання послуг, а також проектування, впровадження, тестування, використання та моніторинг розгорнутих хмар.

2 Дотримання законів, правил, стандартів та специфікацій

2.1 Дотримання міжнародних та державних стандартів, законів і правил.

2.2 Дотримання законів та правил держав, та їх застосування до даних хмари, що фізично розташовуються в межах цієї держави.

2.3 Законодавство в сфері електронних даних.

2.4 Підтримка в проведенні експертизи.

3 Довіра до постачальника послуг

3.1 Доступ до конфіденційної інформації осіб (інсайдерів), завдяки своєму службовому становищу.

3.2 Право власності електронних даних.

3.3 Складені сервіси та сервіси, які використовують сервіси хмари, надані третьою стороною.

3.4 Аудит постачальника, моніторинг, тестування та оновлення програмного та апаратного забезпечення постачальника.

3.5 Захист персональних даних користувача.

3.6 Управління ризиками.

4 Архітектура програмного і апаратного забезпечення

4.1 Зовнішні атаки на інфраструктуру.

4.2 Захист віртуальної мережі.

4.3 Захист образів віртуальних машин.

4.4 Клієнтський захист.

4.5 Захист серверів постачальника.

4.6 Моніторинг захисту.

5 Ідентифікація і управління доступом

5.1 Автентифікація.

5.2 Контроль доступу.

5.3 Спільний доступ до інформації в хмарі.

5.4 Управління ключовими даними.

6 Ізоляція програмного забезпечення

6.1 Складність ОС, програмного чи апаратного забезпечення, призначеного для розміщення та роботи віртуальної машини.

6.2 Загрози, пов'язані з іншими користувачами віртуальних машин.

7 Захист даних

7.1 Концентрація даних.

7.2 Ізоляція даних.

7.3 Безпечне зберігання, відновлення, архівування, видалення даних.

8 Доступність ресурсів та даних

8.1 Відключення хмарних сервісів (тимчасове, тривале, постійне).

8.2 Атаки DDoS.

8.3 Загрози, пов'язані з розташуванням даних.

9 Реагування на інциденти

9.1 Моніторинг наявності та доступності даних.

9.2 Аналіз інцидентів та їх розв'язання.

2.4 Порівняння підходів та сутностей класифікацій ІБ організацій CSA, ENISA, NIST

Порівняння здійснено за трьома основними групами складових: правові, організаційні та технічні питання ІБ у хмарі. Засновуючись на розглянутих класифікаціях, було виділено питання ІБ до кожної з груп, що наведені в таблицях 1, 2 та 3. Якщо питання ІБ було розглянуто в класифікації повністю, воно відмічено як «+», якщо частково – «+/-», в разі відсутності – «-».

Аналіз даних таблиць показує, що в основному складові ІБ збігаються в усіх класифікаціях. Найбільш повна та структурована класифікація була надана організацією CSA, але її недоліком є об'єднання правових та організаційних проблем ІБ. Головною перевагою класифікації ENISA є оцінка ймовірності виникнення ризиків, пов'язаних з ІБ, причинами їх виникнення, взаємозв'язки з іншими ризиками, та їх вплив на систему та її елементи. До недоліків класифікації NIST можна віднести відсутність поділу проблем ІБ на три основних групи, як це було зроблено в класифікації ENISA.

3. АНАЛІЗ ПРОБЛЕМНИХ ПИТАНЬ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРІ

Більшість з проблем захисту інформації користувача в хмарі може бути вирішено з використанням існуючих методів криптографічного захисту інформації, адміністративних мір 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.

Так, наприклад, для забезпечення конфіденційності та цілісності даних, що зберігаються в хмарі, необхідно використовувати алгоритми цифрового підпису та шифрування, які засновані на міжнародних стандартах. Для запобігання несанкціонованого використання профілю користувача можна використовувати існуючі методи двофакторної автентифікації користувача.

Сьогодні 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. Практика в таких питаннях показує, що лише розробка відкритого єдиного міжнародного стандарту може вирішити це питання.

Головними проблемами, які потребують подальшого детального аналізу та вирішення, є такі:

а) Проблема привілегійованих користувачів. Найбільшу загрозу для безпеки інформації в хмарі становлять користувачі, які мають привілегійований доступ до функцій системи або адміністратори хмарних сервісів, тому для зменшення ризику можливих деструктивних дій з їх боку, доцільно вести незалежний нагляд та контроль за їх діями в хмарі. Як показує статистика саме на внутрішніх користувачів припадає найбільша кількість порушень безпеки.

Таблиця 1

Порівняння правових складових ІБ

№	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 авторського права (DRM)	+	-	-
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

№	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	+	+	+

Таблиця 3

Порівняння технічних складових ІБ

№	Технічні питання ІБ		Класифікація		
			CSA	ENISA	NIST
1	Доступність даних та ресурсів	1.1 Відключення хмарних сервісів	+	+	+
		1.2 Атаки DDoS	-	+	+
		1.3 EDoS-атака	-	+	-
		1.4 Розташування даних	+	+	+
		1.5 Вичерпання ресурсів	+	+	-
2	Переносимість та інтероперабельність забезпечення	2.1 Сумісність забезпечення	+	+	+
		2.2 Стандартизований інтерфейс	+	-	-
3	Безпеки додатків та програм	3.1 Безпечність ПЗ	+	+	+
		3.2 Розмежування доступу	+	+	+
		3.3 Моніторинг активності додатків	+	+	+
		3.4 Виявлення небезпечних програм	+	+	+
		3.5 Захист образів віртуальних машин від модифікації	+	-	+
4	Управління даними та захист	4.1 Ізоляція даних	+	+	+
		4.2 Безпечне зберігання та оброблення даних	+	+	+
		4.3 Шифрування даних	+	+	+
		4.4 Управління ключами	+	+	+
5	Ідентифікація, автентифікація та управляння доступом	5.1 Моделі ідентифікації та автентифікація в хмарі	+	-	-
		5.2 Керування профілями користувачів у хмарі	+	+	+
		5.3 Надання послуг ідентифікації, автентифікації, спільного доступу до інформації в хмарі або ресурсів	+	+	+
		5.4 Реалізація ідентифікації користувачів	+	+/-	+
		5.5 Доступ до даних авторизованих користувачів	+	+	+
6	Віртуалізація	6.1 Забезпечення захисту гістьової віртуальної машини від атак	+	-	+
		6.2 Механізми захисту від неправомірних дій адміністраторів	+	+	+
		6.3 Питання швидкодії, пікового збільшення навантаження, збільшення числа вузлів	+	+	+
		6.4 Забезпечення безпеки даних на рівні віртуальної машини	+	-	+

б) Однією з головних проблем, що гальмує поширення хмарних обчислень, є невідповідність законів у сфері обробки, передачі, збереження та захисту інформації різних держав. Вирішення цієї проблеми є ключовим фактором для можливості фізичного розміщення серверів постачальника хмарних сервісів у різних країнах та регіонах, а також використанням користувачами з різних країн одного постачальника послуг. Ця проблема найбільш істотно торкатиметься транснаціональних корпорацій.

в) Питання довіри до постачальника послуг можуть бути вирішені лише за рахунок проведення аудиту безпеки постачальника хмарних послуг та перевірки відповідності його системи безпеки міжнародним вимогам до захисту інформації, що сформульовані в міжнародних стандартах. Формулювання та обґрунтування вимог є одним з важливих питань.

г) Питання загальних вразливостей у хмарі практично нічим не відрізняються від аналогічних у традиційних системах, за винятком того, що знайдена одна вразливість може бути використана для всієї хмари, але водночас її можна легше виправити за допомогою централізованого оновлення, на відміну від традиційних систем. І в цей час її критичність набагато більша, бо вона може з легкістю уразити всіх користувачів даного постачальника послуг, тому потребує превентивних мір та засобів захисту.

д) Проблеми доступності до сервісів та даних користувачами, відновлення їх роботи після збоїв, чи втрати даних повинні вирішуватися на адміністративному та правовому рівнях. При укладанні договорів з користувачем мають бути чітко визначені обов'язки сторін та міра їх відповідальності в залежності від обставин події, що призвела до цих наслідків, а розслідування повинна проводити третя незалежна сторона. Аналогічна проблема існує і в традиційних системах, але користувач має можливість безпосередньо впливати на рівень резервування в системі, що дає можливість більш гнучко її налаштовувати під конкретні вимоги користувача та його фінансові можливості.

є) Проблема надання доступу, спільного доступу та блокування доступу до ресурсів і даних у хмарі користувачам.

е) Проблема захисту інтелектуальної власності в хмарі, зокрема програмного забезпечення та даних.

4. ПЕРЕВАГИ ТА НЕДОЛІКИ ВИКОРИСТАННЯ ХМАР

Головною перевагою використання хмарних обчислень, яка покладена в основу технології,

є балансування робочого навантаження, за рахунок чого досягається більш ефективне використання ресурсів обчислювальної системи. До основних переваг технології можна віднести:

– можливість доступу до ресурсів у хмарі, використовуючи Інтернет з'єднання, звичайний браузер та невимогливий до ресурсів термінал кінцевого користувача;

– швидке розгортання власних сервісів та/або збільшення робочого навантаження на існуючі постачальником хмарних послуг;

– підтримка резервування, самовідновлення та масштабування, яке дозволяє підвищувати надійність системи та зменшувати ризики при відмовах програмного та апаратного забезпечення;

– управління робочими навантаженнями в реальному часі, в тому числі пакетними операціями та фоновими програми, що взаємодіють з користувачами;

– моніторинг у реальному часі завантаження та балансу системи, а також виділення ресурсів.

Крім перелічених переваг існують недоліки та проблемні питання, які гальмують впровадження хмарних обчислень, а саме:

– неможливість роботи з сервісами хмари без постійного підключення до Інтернет;

– складний або неможливий процес переходу від одного постачальника хмарних послуг до іншого;

– відсутність єдиного міжнародного правового регулювання у сфері хмарних обчислень та обробки інформації в хмарі;

– довіра до постачальника послуг користувачів;

– питання захисту інформації користувача, що обробляються та зберігаються в хмарі.

Для забезпечення безпеки інформації, хмарні обчислення надають такі переваги:

– спеціалізований персонал: провайдер хмари, як велика організація, для забезпечення безпеки в хмарі наймає спеціалістів у галузі безпеки інформації, що дозволяє співробітникам зосередитися виключно на питанні безпеки, досягти високого рівня безпеки, який не можливо досягти в невеликій організації;

– централізоване керування, конфігурація системи безпеки та її аудит;

– стійкість платформи: апаратний та програмний склад платформи, на якій розгорнуто хмару більш рівномірно, ніж у більшості традиційних обчислювальних центрів, що дозволяє краще автоматизувати діяльність щодо забезпечення безпеки, тестування та виправлення помилок у компонентах платформи;

– наявність ресурсів: можливість динамічного масштабування ресурсів системи, а також резервування та аварійного відновлення, що може бути використано для підвищення стійкості системи проти атак типу «відмова в обслуговуванні», а також швидкого відновлення після серйозних інцидентів;

– резервне копіювання і відновлення: провайдер хмарних послуг може дозволити надання більш високого рівня резервного копіювання і відновлення, ніж той, що забезпечують традиційні центри обробки даних, а також забезпечити зберігання резервних копій за географічною вимогою;

– мобільність кінцевих клієнтів: завдяки архітектурі хмари клієнти можуть використовувати різноманітні портативні пристрої, з невеликою обчислювальною потужністю, виходом до мережі Інтернет, браузером та/або декількома встановленими додатками, щоб отримати доступ до основних обчислювальних ресурсів;

– концентрація даних: використання хмари, як єдиного місця для зберігання та обробки даних, у деяких випадках дозволяє підвищити безпеку, ніж зберігання даних, що розосереджені по портативних комп'ютерах, вбудованих пристроях або зберігаються на знімному носії.

До недоліків використання хмарних обчислень з точки зору безпеки інформації відносять:

– складність системи: загальна хмара є надзвичайно складною порівняно з традиційним центром обробки даних. Велика кількість компонентів, з яких складається хмара, дозволяє проводити атаки на різних рівнях абстракції. Крім компонентів для загальних обчислень, таких як розгортання додатків, віртуальних моніторів машини, гістьових віртуальних машин, зберігання даних є також компоненти, які включають в себе елементи управління: самообслуговування, ресурс обліку, управління квотами, реплікація даних і відновлення, моніторинг рівня сервісу, управління робочим навантаженням.

Загальне багатокористувальницьке середовище: основним недоліком публічних хмар є те, що ресурси та компоненти користувачі поділяють з користувачами, які їм не відомі на логічному рівні, що дозволяє зловмиснику, використовуючи вразливості всередині хмари, подолати механізм розподілу ресурсів між користувачами та отримати несанкціонований доступ до ресурсів.

Однорідність програмного та апаратного складу платформи означає, що єдиний недолік проявлятиметься у всій хмарі та потенційно впливатиме на усіх користувачів послуг

Використання Інтернету: сервіси хмари, а також адміністрування та керування налаштуваннями хмарних сервісів та додатків, використовує незахищену мережу Інтернет. При переході організації на використання хмарних обчислень, для внутрішніх захищених мереж та ресурсів виникають нові інформаційні небезпеки, які слід вирішувати. Також виникає необхідність віддаленого адміністрування з використанням незахищеного каналу передачі інформації.

Втрата контролю: при використанні сервісів хмари, користувач передає контроль над інформацією провайдеру хмари, що несе в собі додаткові ризики для безпеки інформації. Користувач стає залежним від провайдера хмари, та може втратити не тільки логічний контроль над інформацією, але й фізичний.

ВИСНОВКИ

Хмарні обчислення є комбінацією з декількох ключових технологій, які були розроблені протягом багатьох років та розглядаються багатьма дослідниками як наступне покоління IT-архітектури підприємств.

Зі всією сукупністю переваг, які надає використання хмарних обчислень, є багато питань безпеки, які на сьогодні не достатньо добре проаналізовані та знаходяться ще на стадії обговорення.

Як було показано в статті, головною проблемою, що не вирішена в галузі хмарних обчислень на сьогодні, є довіра користувачів до постачальника послуг. Ця проблема гостро стоїть не тільки для компаній та підприємств, що використовують сторонніх постачальників, але й звичайних користувачів, персональні дані яких також потребують захисту та гарантій безпеки. Якщо у випадку великого підприємства воно може захистити себе від загроз проведенням аудиту безпеки провайдера хмарних послуг та аналізом ризиків та загроз інформаційної безпеки, а також застрахувати їх, чи створити свою власну приватну хмару, то невеликі компанії або звичайні користувачі не мають такої можливості. Тому необхідно впроваджувати механізми контролю постачальників хмарних послуг на міжнародному рівні або на рівні держави, з метою проведення аудиту безпеки та перевірки їх відповідності міжнародним або державним стандартам та висунутим до них умов.

У подальших роботах планується розглянути та проаналізувати існуючі архітектури побудови хмар з точки зору їх безпеки.

Література

[1] The NIST Definition of Cloud Computing, NIST Special Publication 800-145, 2011.

[2] Guidelines on Security and Privacy in Public Cloud Computing , NIST SP800-144, 2011.

[3] Cloud Computing Synopsis and Recommendations DRAFT, NIST, 2011.

[4] Security Guidance for Critical Areas of Focus in Cloud Computing, Version 3.0. Technical report, Cloud Security Alliance, 2011. Режим доступу http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

[5] D. Catteddu and G. Hogben. Cloud Computing Security Risk Assessment. Technical report, European Network and Information Security Agency, November 2009. Режим доступу http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-risk-assessment

[6] D. Catteddu and G. Hogben. Cloud Computing Information Assurance Framework. Technical report, European Network and Information Security Agency, November 2009. Режим доступу http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework

[7] Wayne Jansen, Timothy Grance Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144, 2011. Режим доступу http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[8] Lee Badger Cloud Computing Synopsis and Recommendations NIST Special Publication 800-146 Lee Badger, Tim Grance, Robert Patt-Corner, Jeff Voas, 2012. Режим доступу http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf

Надійшла до редколегії 19.03.2013

Аулов Іван Федорович, аспірант кафедри БІТ ХНУРЕ. Наукові інтереси: дослідження принципів побудови, розгортання і аналіз стійкості асиметричних криптографічних систем, хмарні та мобільні технології.

Горбенко Іван Дмитрович, доктор технічних наук, професор, завідувач кафедри БІТ ХНУРЕ, головний конструктор АТ «Інститут інформаційних технологій». Наукові інтереси: прикладна криптологія, криптографічні системи та протоколи, проектування та розробка систем, комплексів та засобів криптографічного захисту інформації.

УДК 004.75:004.05

Облачные вычисления и анализ информационной безопасности в облаке / И.Ф. Аулов, И.Д. Горбенко // Прикладная радиоэлектроника: науч.-техн. журнал. – 2013. – Том 12. – № 2. – С. 194–201.

В статье рассматривается современное состояние облачных вычислений, преимущества и недостатки их использования для предприятия, государства и научной деятельности. Определяются и анализируются стандарты, нормативные и руководящие документы в области информационной безопасности облачных вычислений, которые разработаны Cloud Security Alliance (CSA), Европейским агентством сетевой и информационной безопасности (ENISA) и Национальным институтом стандартов и технологий (NIST), а также приводятся результаты детального анализа вопросов информационной безопасности в облаке.

Ключевые слова: облачные вычисления, информационная безопасность, сравнительный анализ, преимущества и недостатки вычислений в облаке.

Табл.: 3. Библиогр.: 8 назв.

UDC 004.75:004.05

Cloud computing and analysis of information security in the cloud / I.F. Aulov, I.D. Gorbenko // Applied Radio Electronics: Sci. Journ. – 2013. – Vol. 12. – № 2. – P. 194–201.

The paper considers the current state of cloud computing, the advantages and disadvantages of using them for business, government and academia, analyzes the standards, regulations and guidelines on information security of cloud computing developed by Cloud Security Alliance (CSA), the European Agency for Network and Information Security (ENISA) and the National Institute of Standards and Technology (NIST), for detailed analysis of information security issues in the cloud.

Keywords: cloud computing, information security, comparative analysis, advantages and disadvantages of cloud computing.

Tab.: 03. Ref.: 08 items.