УДК 004.738.5

Т.Г. Білова, В.О. Ярута, І.О. Побіженко

Харківська державна академія культури, Харків

АНАЛІЗ РИЗИКІВ РЕФЕРЕНТНОЇ СТРУКТУРИ ХМАРНИХ ОБЧИСЛЕНЬ

Проаналізовано референтну структуру хмарних обчислень, яка зв'язує сервісні моделі, моделі розгортання та основні характеристики технології. Для основних суб'єктів хмарних обчислень визначені ролі, функції та відношення з іншими суб'єктами. Розглянуті типові сценарії взаємодії в рамках хмарних відношень, проведено аналіз їх переваг та недоліків.

***Ключові слова**: хмарні технології, референтна структура, сервісна модель, модель розгортання.*

Вступ

Хмарні технології – віртуальне середовище для зберігання та обробки інформації, що об'єднує в собі апаратні засоби, ліцензійне програмне забезпечення, канали зв'язку та технічну підтримку користувачів. Основними перевагами хмарних обчислень є незалежність від програмної платформи і географічного розташування, а також можливість масштабованості. Але є проблеми, пов'язані з надійністю зберігання даних, необхідністю законодавчого регулювання та ін., які стримують потенційних користувачів від переносу своїх ресурсів до хмари [1, 2].

Хмарні обчислення є новітньою концепцією, яка потребує уніфікації та стандартизації основних понять та визначення оптимальних сценаріїв використання. Тому актуальним є розробка базових принципів використання цих технологій, яка дозволить користувачу зорієнтуватися у різноманітті запропонованих послуг та мінімізувати ризики від їх використання.

Узагальнення необхідних термінів та зв'язків між суб'єктами хмарних обчислень зручно аналізувати з допомогою референтної структури [3], що представляє собою високорівневий погляд на хмарні обчислення. Але відношення між суб'єктами моделі потребує подальшої розробки та уточнення.

Мета та завдання дослідження. *Метою* даного дослідження є аналіз ризиків референтної структури хмарних обчислень та визначення найбільш ефективних сценаріїв їх використання.

У відповідності з поставленою метою слід вирішити наступні *завдання*: проаналізувати референтну структуру хмарних обчислень; дослідити відношення між суб'єктами хмарних обчислень; визначити ролі та функції кожного з суб'єктів та ризики реалізації типових сценаріїв хмарних відношень.

Основна частина

Референтна структура хмарних обчислень обговорюється як дорожня карта для розуміння, вибору, проектування та розгортання хмарної інфраструктури. Вона зв'язує різні хмарні сервіси та відображає їх на загальну модель, яка містить основні поняття технології та відносини між ними.

Референтна архітектура хмарних обчислень NIST, запропонована в [3], представляється у вигляді ієрархічних діаграм, на кожній із яких збільшується рівень деталізації. Вона містить три рівні:

– три сервісних моделі (SaaS, PaaS, IaaS);

– чотири моделі розгортання (private cloud, community cloud, public cloud, hybrid cloud);

– п'ять основних характеристик (on-demand self-service / broad network access / resource pooling / rapid elasticity / measured service).

В табл. 1 представлено п'ять головних діючих суб'єктів – акторів (actors), що взаємодіють у рамках хмарної інфраструктури.

Таблиця 1

Суб'єкти хмарних обчислень

Суб'єкт	Визначення
Хмарний споживач Cloud Consumer	Особа або організація, що підтримує бізнес-відносини і що використовує послуги хмарних провайдерів.
Хмарний провайдер Cloud Provider	Особа, організація або сутність, що відповідає за доступність хмарної послуги для споживачів.
Хмарний брокер Cloud Broker	Сутність, керуюча використанням, продуктивністю і наданням хмарних послуг, а також встановлює відносини між провайдерами і споживачами.
Хмарний аудитор Cloud Auditor	Учасник, який виконує незалежну оцінку хмарних послуг, обслуговування інформаційних систем, продуктивності та безпеки реалізації хмари.
Хмарний оператор зв'язку Cloud Carrier	Посередник, що надає послуги підключення і доставки хмарних послуг від провайдера до споживача.

Згідно з референтною структурою кожен суб-'єкт виступає в ролі (role) і виконує дії (activities) і функції (functions).

Хмарних споживачів можна розділити на три групи згідно з моделлю обслуговування, яку вони використовують:

1. SaaS – бізнес-користувачі та адміністратори прикладань (автоматизація бізнес-процесів).

2. PaaS – розробники прикладань, тестувальники (розробка, тестування та управляння прикладаннями в хмарному середовищі).

3. IaaS – системні розробники, адміністратори, IT-менеджери (створення та встановлення, керування та моніторинг сервісів для управління IT-структурою).

Кожна група вимагає відповідних послуг, найбільш затребуваними є безпека, конфіденційність та надійність зберігання та обробки даних.

Хмарний провайдер відповідає за доступність послуг та підтримує наступну діяльність:

1. Розгортання сервісів (моделі private cloud, community cloud, public cloud, hybrid cloud).

2. Оркестрація сервісів – систематизація, координація та управління хмарної інфраструктурою. Складається з наступних концептуальних рівнів:

– рівень сервісу (Service Layer) визначає базові сервіси, що надаються хмарним провайдером;

– рівень абстракції і контролю ресурсів (Resource Abstraction and Control Level) призначає елементи програмного забезпечення (гипервізор, віртуальні сховища даних) і підтримує програмні компоненти, що використовуються для реалізації хмарної інфраструктури, надає асоційовані функціональні модулі, які керують абстрагованими ресурсами для забезпечення ефективного, безпечного і надійного використання;

– рівень фізичних ресурсів (Physical Resource Level) включає комп'ютерне обладнання та інженерну інфраструктуру.

3. Хмарний сервіс-менеджмент (Cloud Service Management) включає наступні функції, необхідні для управління і функціонування хмарних сервісів:

– підтримка бізнесу (Business Support) – набір сервісів, пов'язаних з бізнесом і орієнтованих на роботу з клієнтами і підтримуючими процесами, такими як розміщення замовлень, обробку рахунків та збір платежів;

– просування / конфігурування (Provisioning / Configuration) містить функції, необхідні для управління і функціонування сервісів (автоматичне розгортання, модифікація ресурсів, моніторинг та звітність, вимірювання показників, управління рівнем обслуговування);

– портіруємість (Portability) як можливість перенесення даних з однієї системи в іншу без необхідності повторного створення або ведення описів даних чи їх значної модифікації переносити додатки або можливість програмного забезпечення виконуватися на більш ніж одному типі комп'ютеру під більш ніж однією операційною системою;

– інтероперабельність (Interoperability) – можливість взаємодіяти, виконувати програми або передавати дані між різними функціональними одиницями відповідно до заданих умов.

4. Безпека (Security) містить наступні функції:

– аутентифікація та авторизація (Authentication and Authorization) хмарних споживачів з використанням попередньо створеного мандата доступу;

– доступність (Availability) – налаштування конфігурацій та призначення ресурсів для відновлення і підключення нових вузлів в хмару;

– конфіденційність (Confidentiality) – виявлення та моніторинг віртуальних ресурсів, моніторинг функціонування хмари і генерація звітів про продуктивність;

– управління ідентифікацією (Identity management) як надання можливостей кількісних вимірів на рівні абстракції відповідному типу сервісу (засобів зберігання, обробки, пропускної здатності та активних облікових записів користувачів);.

– моніторинг безпеки та обробка інцидентів (Security monitoring & Incident Response) – визначення параметрів SLA контракту та моніторинг виконання SLA;

– управління політикою безпеки (Security policy management) – генерація, застосування, аудит та оновлення політик безпеки для споживачів;

– приватність (Prrivacy) захищає достовірні, належні і відповідні збір, обробку, передачу, використання і зберігання в хмарі персональних даних та інформації, що дозволяє ідентифікувати особу.

Найбільш критичними в хмарних технологіях є проблеми безпеки даних, але не менш важливими є наявність/відсутність функцій портіруємості даних. Для споживачів потрібно забезпечувати наступні функції:

– копіювання даних з/в хмару;

– пакетний перенос даних з використанням диску;

– перенесення образів віртуальних машин – міграція примірника або образу віртуальної машини від одного провайдера до іншого;

– міграція додатків (сервісів) від одного сервіс-провайдера до іншого.

Підвищення рівня довіри споживачів до провайдерів досягається за рахунок введення проміжних суб'єктів в хмарних обчисленнях – аудиторів та брокерів.

Хмарний аудитор виконує незалежну оцінку хмарних послуг, обслуговування інформаційних систем, продуктивності та безпеки реалізації хмари. Цей суб'єкт може давати оцінку сервісів, що нада-

ються хмарним провайдером, в термінах контролю безпеки, дотримання приватності, продуктивності та ін. Для аудиту безпеки хмарний аудитор може проводити оцінку контролю безпеки інформаційної системи з метою визначення меж, для яких контроль виконується відповідним чином, система функціонує за призначенням і виробляє результат відповідно до вимог безпеки, що пред'являють до системи.

Функції хмарного аудитора роблять більш прозорим та керованим діяльність провайдера та дозволяють споживачу оцінити рівень хмарних послуг та отримати надійну інформацію про можливі ризики.

У ході еволюції хмарних обчислень інтеграція хмарних сервісів стає занадто складною для управління. Для вирішення цієї проблеми споживачі можуть звернутися до послуг хмарного брокера. Цей суб'єкт керує використанням, продуктивністю і наданням хмарних послуг, а також встановлює відносини між провайдерами і споживачами.

Основні послуги хмарних брокерів:

1. Сервісне посередництво (Service Intermediation) полягає у розширенні заданого сервісу, розвитку його окремих функцій та наданні додаткових сервісів хмарним споживачам.

2. Агрегування сервісів (Service Aggregation) – комбінація і інтеграція окремих сервісів в один і більше сервісів, інтеграція даних і їх безпечне перенесення між хмарним споживачем і хмарними провайдерами.

3. Арбітраж сервісів (Service Arbitrage) аналогічний агрегуванню, але відрізняється тим, що послуги не модифікуються. Забезпечує хмарному брокеру гнучкий і вигідний вибір для пропозиції хмарним споживачам.

Ще одним посередником між споживачем та провайдером виступає хмарний оператор зв'язку. Він надає послуги підключення і транспорт хмарних послуг від провайдерів до споживачів через мережеві, телекомунікаційні та інші пристрої доступу (комп'ютери, ноутбуки, мобільні телефони та ін.)

Доставка послуг і пристроїв може забезпечуватися мережевими та телекомунікаційними операторами, а також транспортними агентами. Транспортний агент – бізнес-організація, що забезпечує фізичне транспортування засобів зберігання інформації, таких як жорсткі диски підвищеної ємності.

Хмарний провайдер повинен укладати з хмарним оператором зв'язку угоду про рівень обслуговування (SLA) для забезпечення відповідного рівня сервісу. У загальному випадку, до хмарного оператора зв'язку можуть пред'являтися вимоги щодо надання виділеного і захищеного з'єднання.

Відношення між хмарними суб'єктами визначаються типовими сценаріями використання:

1. Хмарний споживач запрошує послугу у хмарного брокера. Хмарний брокер може створити новий сервіс, комбінуючи набір сервісів або розширюючи існуючий сервіс. У цьому випадку хмарний провайдер невидимий хмарному споживачеві.

2. Хмарний оператор зв'язку представляє послуги підключення і доставку хмарних послуг від хмарного провайдера хмарному споживачеві. Хмарний провайдер встановлює угоду про рівень обслуговування з хмарним оператором і може запитувати виділені і захищені з'єднання.

3. Хмарний аудитор проводить незалежну оцінку обслуговування та безпеки реалізації хмарної послуги.

Незалежно від використовуваного сценарію, можна виділити першочергові вимоги споживачів до рівня потрібного сервісу:

1. Надійність та захищеність доступу.

2. Місце виконання робочих загрузок призначується динамічно та скрито від споживачів – загрузки повинні автоматично мігрувати між фізичними вузлами хмари.

3. Усунення ризиків множинної оренди – робочі навантаження різних споживачів можуть виконуватися одночасно на одних і тих же хмарних системах, будучи розділеними тільки за допомогою політик доступу, визначених на рівні програмного забезпечення провайдера. Слабі місця в цьому програмному забезпеченні або в політиках можуть нанести втрату безпеки споживача.

4. Імпорт / експорт даних і обмеження можливості їх виконання – тимчасові характеристики пакетного імпорту та експорту даних можуть перевищити можливості мережі. Робота в режимі реального часу або обробка критично важливих запитів можуть виявитися проблематичними через мережеві затримки і інші обмеження.

Споживачі хмарних обчислень повинні оцінювати наслідки порушення будь-якого з вимог для своєї бізнес-моделі і впливу на досягнення довгострокових цілей. Організації, які обговорюють застосування хмар, мають детально розглядати аспекти використання різних хмарних сценаріїв.

При порівнянні використання хмар з традиційною моделлю "внутрішніх" обчислень, хмарна модель вимагає від споживачів передачі провайдеру двох важливих функцій, які передбачають високий рівень довіри:

– контролю – можливості надавати права доступу до даних і програм, і виконувати дії (такі як стирання даних або відключення від мережі), які можуть не відповідати намірам споживача;

– явності дій – можливості здійснення моніторингу статусу програм і даних споживача і того, як до них здійснюється доступ.

Однак, межі контролю і видимості, які необхідно передати провайдеру, залежать від багатьох факторів, включаючи фізичне володіння і можли-

вість конфігурації (з високим рівнем довіри) механізмів захисту кордонів доступу до обчислювальних ресурсів споживача.

Ключова концепція комп'ютерної безпеки – периметр безпеки (security perimeter).

Периметр безпеки виконує роль бар'єру відносно операцій доступу: сутності, які знаходяться всередині периметра, можуть здійснювати вільний доступ до ресурсів, що знаходяться тільки всередині периметра.

Однак, сутності, що знаходяться за межами периметра, можуть отримувати доступ до ресурсів усередині периметра якщо тільки це дозволено засобами контролю кордонів (boundary controller) на основі застосування відповідних політик доступу.

Кожна модель розгортання хмар формує свій периметр безпеки – власний (on-site) або на аутсоурсінге (outsourced). Найбільш складною є гібридна модель, яка є комбінацією інших моделей. Тому гібридне розгортання може припускати і вплив на периметр безпеки його елементів - "будівельних блоків", і унікальні аспекти впливу, що виникають в результаті об'єднання безлічі систем в більш комплексні інтегровані системи.

Таким чином, найбільш ефективні способи захисту інформації в хмарних технологіях [4]:

1. Шифрування - один з найефективніших способів захисту даних. Провайдер, що надає доступ до даних повинен шифрувати інформацію клієнта, а також у випадку відсутності необхідності, безповоротно видаляти.

2. Захист даних при передачі шляхом шифрування. Такі дані повинні бути доступні тільки після аутентифікації.

3. Аутентифікація - захист паролем. Для забезпечення більш високої надійності використовуються токени і сертифікати.

4. Ізоляція користувачів – використання індивідуальної віртуальної машини і віртуальної мережі.

Висновки

Референтна структура хмарних обчислень визначає стандарти в області хмарних технологій та інформаційної безпеки, фундамент і концептуальну основу, а також підходи до теорії та практичного забезпечення ефективної обробки даних хмарних споживачів.

Посередниками між хмарними споживачами та провайдерами виступають проміжні суб'єкти – аудитори, брокери та оператори зв'язку, які допомагають оцінити рівень надання послуг, створити найбільш відповідаючи вимогам сервіси та організувати к ним надійний доступ. Типові сценарії організації хмарних обчислень дозволяють знизити ризики втрати даних та забезпечують потрібний рівень надійності та конфедеційності обробки даних в хмарі.

Подальші дослідження у даному напрямі повинні охоплювати питання організації периметрів безпеки для кожної із моделей розгортання хмар та у випадку їх інтеграції в гібридну хмару.

Список літератури

1. Білова Т. Г. Перспективи використання хмарних технологій в системах електронного документообігу / Т. Г. Білова, В. О. Ярута [Текст] // Системи обробки інформації. – Х., 2014. – Вип. 4 (120). – С. 86–89.

2. Белова Т. Г. Анализ проблем доверия в облачных технологиях [Текст] / Т. Г. Белова, И. А. Побеженко, В. В. Побеженко // Східно-Європейський журнал передових технологій. — Х., 2013. — № 2 (62). — С. 59–62.

3. Основы Облачных вычислений (по рекомендациям NIST) [Электронный ресурс]. – Режим доступа: http://cloud.sorlik.ru/definition.html.

4. Угрозы облачных вычислений и методы их защиты [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/183168.

Надійшла до редколегії 2.09.2014

Рецензент: д-р техн. наук проф. Г.Г. Асєєв, Харківська державна академія культури, Харків.

АНАЛИЗ РИСКОВ РЕФЕРЕНТНОЙ СТРУКТУРЫ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ

Т.Г. Белова, В.А. Ярута, И.А. Побеженко

Проведен анализ референтной структуры облачных вычислений, связывающей сервисные модели, модели развертывания и основные характеристики технологии. Для основных субъектов облачных вычислений определены роли, функции и отношения с другими субъектами. Рассмотрены типичные сценарии взаимодействия в рамках облачных отношений, выделены их преимущества и недостатки.

Ключевые слова: *облачные технологии, референтная структура, сервисная модель, модель развертывания.*

RISK ANALYSIS OF THE REFERENCE ARCHITECTURE CLOUD COMPUTING

T.G. Belova, V.O. Yaruta, I.O. Pobizhenko

The analysis of the reference structure of cloud computing, linking service models, deployment models and the basic characteristics of the technology. For the main subjects of cloud computing defined roles, functions and relationships with other entities. Consider a typical scenario of interaction within the cloud relations, highlighting their advantages and disadvantages.

Keywords: *cloud computing, reference architecture, service models, deployment models.*