УДК 004.75:004.05

І.Д. ГОРБЕНКО, д-р техн. наук, М.І. ХАРЛАМБ

СТВОРЕННЯ ТА АНАЛІЗ МОДЕЛІ ЗАГРОЗ ПРИ ОБЧИСЛЕННЯХ В ХМАРІ

Вступ

Технологія хмарних обчислень є одним з найбільш перспективних напрямів розвитку інформаційних технологій з тих, що в даний час розглядаються в якості альтернативи традиційній моделі обробки інформації. Використання хмарних обчислень дозволяє реалізувати можливість віддаленої обробки інформації, забезпечує досягнення високих показників відмовостійкості та доступності інформаційної інфраструктури.

Хмарні обчислення – модель забезпечення повсюдного та зручного доступу через мережу до спільного пулу обчислюваних ресурсів, що підлягають налаштуванню, які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними затратами або зверненням до провайдера [1]. Одними з головних переваг використання хмарних обчислень можна назвати балансування робочого навантаження, що покладено в основу технології,використання розповсюджених та доступних засобів для доступу до ресурсів хмари, швидке розгортання власних сервісів, підтримка різноманітних можливостей пов’язаних із обробкою та зберіганням даних. Ця перевага забезпечує досягання більш ефективного використання ресурсів системи [1].

Разом з цим переваги використання наведеної технології призводять до виникнення нових актуальних загроз інформаційній безпеці, пов’язані перш за все із зниженням рівня контрольованості процесів обробки інформації та з динамічністю моделі надання ресурсів, про що також визначалось в [1]. Так, при використанні систем хмарних обчислень у споживача відсутня можливість застосування додаткових засобів обмеження доступу до інформації, таких як контроль фізичного доступу та інших організаційних і технічних заходів [1]. Актуальність роботи також пов’язана з тим, що досі немає чіткої та офіційно визначеної моделі загроз для хмарних обчислень. Незважаючи на те, що федерація CSA (CloudSecurityAlliance) дуже ретельно займається питаннями безпеки у хмарі, останні додатки до моделі загроз в їх редакції датовані 2010 роком, що станом на теперішній час є застарілими даними [3, 7].

Таким чином, питання забезпечення інформаційної безпеки при використанні технології хмарних обчислень стає актуальним з її поширенням та повсюдним впровадженням. Адекватність розглядання цього питання в термінах безпеки інформаційної інфраструктури можна обґрунтувати тим, що вже існують деякі механізми, що дають можливість створення безпечного простору для роботи з хмарними технологіями, їх опис та відповідні заходи розглядаються нижче [1].

1. Загальна модель взаємодії частинн системи хмари

Якщо розглядати технологію хмарних обчислень як частину інформаційної інфраструктури, необхідно визначити, що головним питанням стає забезпечення конфіденційності, цілісності та доступності оброблюваної інформації. Для того щоб більш детально вивчити проблеми пов’язані з цими питаннями, треба розглянути структуру будування системи хмари (рис.1).

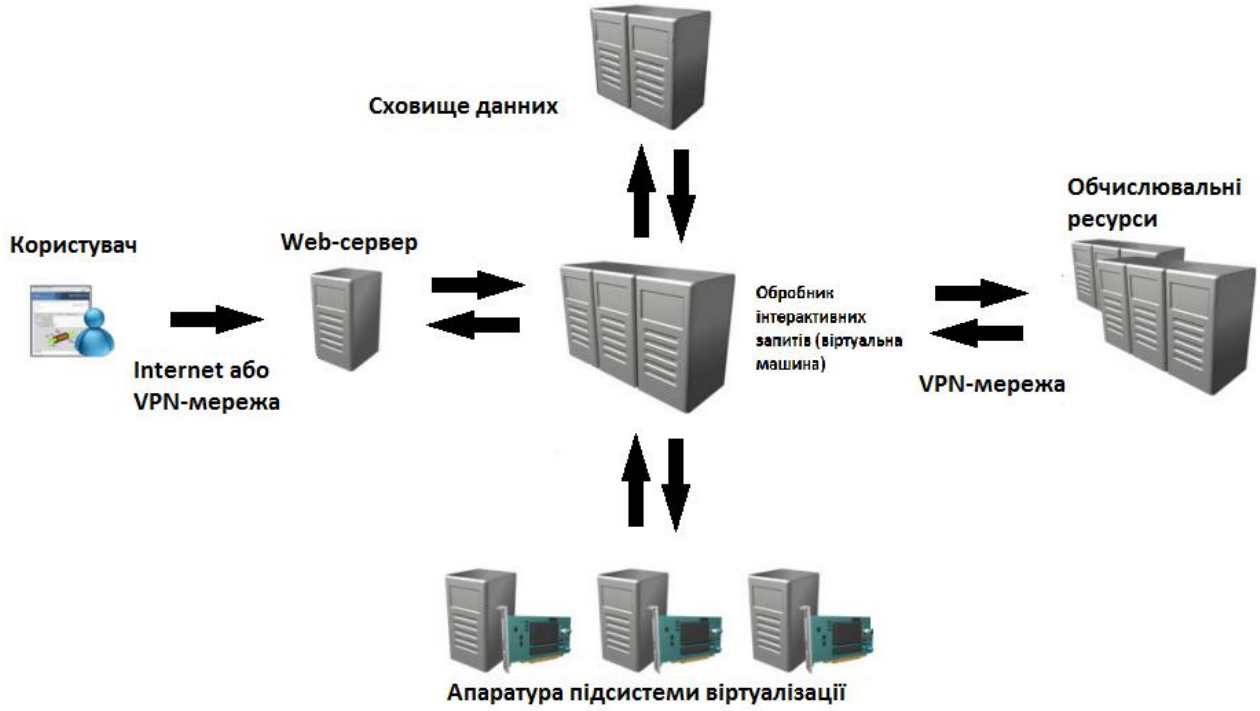

Рис. 1. Загальна структура побудування системи хмари

Таким чином, виходячи із поданої структури, формально можна виділити декілька частин, з яких складається система хмари: користувацька сторона (ПЗ та апаратне забезпечення), мережа з'єднання із Web-сервером, обробник інтерактивних запитів, апаратура підсистеми віртуалізації, сховище даних, обчислювальні ресурси, внутрішня мережа системи хмари.

2. Існуючі механізми забезпечення безпеки інформації в хмарі

Питання захисту інформації в хмарі виникло разом з розвитком цієї технології, тому вже існують деякі механізми, що дають можливість створення безпечного простору для роботи з хмарними технологіями, їх опис та відповідні заходи наведено у табл.1.

Таблиця 1

Механізми забезпечення безпеки інформації в хмарі	Засоби забезпечення (відповідно до механізму)
Існування спеціалізованого персоналу(частіше за все провідні спеціалісти у галузі інформаційної безпеки).	Встановлення відповідного регламенту до прийняття на роботу спеціалізованого персоналу, контроль за діяльністю спеціалістів.
Можливість забезпечення централізованого керування, конфігурації системи безпеки та її аудиту.	Встановлення керівників та адміністраторів систем, використання спеціалізованих програм аудиту та конфігурації системи встановленого політикою безпеки чи іншим офіційним документом зразка[5].
Досконалість апаратного та програмного складу платформи, на якій розгорнуто хмару, високий рівень рівномірності , ніж у більшості традиційних обчислювальних центрів, що дозволяє краще автоматизувати діяльність по забезпеченню безпеки, тестування та виправлення помилок в компонентах платформи.	Використання новітнього апаратного забезпечення та ліцензованого програмного забезпечення з додержанням до певних рекомендацій з експлуатації.
Наявність ресурсів: можливість динамічного масштабування ресурсів системи, а також резервування та аварійного відновлення.	Забезпечення стійкого апаратного забезпечення та налагодженої системи резервного копіювання[3].
Резервне копіювання і відновлення.	Забезпечення великих об'ємів ресурсів для резервування, наявність спеціального програмного забезпе-

	чення.

Продовження табл. 1

Концентрація даних: використання хмари, як єдиного місця для зберігання та обробки даних в деяких випадках дозволяє підвищити безпеку, ніж зберігання даних, що розосереджені по портативним комп'ютерам, вбудованим пристроям або зберігаються на знімному носії.	Використання спеціалізованих кластерів для зберігання даних.

Відповідно до табл.1 можна зробити висновок, що наведені механізми і засоби забезпечення безпеки інформації не є досконалими, тому потрібно проектувати і розробляти такі системи, які будуть спроможні забезпечити певний рівень захисту системи від можливих загроз [2, 6].

3. Слабкі місця використання хмарних обчислень відносно інформаційної безпеки

Для того щоб провести аналіз можливих уразливостей системи хмарних обчислень та скласти її модель загроз, потрібно в першу чергу виявити витоки їх постання. До основних причин виникнення уразливостей систем 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;

– загальне багатокористувацьке середовище: основний недолік публічних хмар є те, що ресурси та компоненти користувачі поділяють з користувачами, які їм невідомі 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 буде проявлятися у всій хмарі та потенційно впливати на усіх користувачів послуг;

– використання Інтернету: сервіси хмари, а також адміністрування та керування налаштуваннями хмарних сервісів та додатків, використовує незахищену мережу Інтернет;

– 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.

Таким чином, на основі виявлених причин виникнення загроз можна комплексно розробляти та аналізувати модель загроз системи хмарних обчислень [1, 2, 7].

4. Модель загроз при обчисленнях в хмарах

Для того щоб детально вивчити можливі загрози в системі хмарних обчислень та скласти відповідну модель, необхідно окремо розглянути кожну частину системи та виявити певні уразливості. Посилаючись на рис.2 та порядок розділення системи на конкретні частини (з першого розділу), можна виділити наступні частини та відповідні загрози:

1. A1 – атака на рівні користувача. Можливі загрози:

✓загрози[1] на рівні програмного забезпечення (шпигунське програмне забезпечення, використання уразливостей операційної системи, віруси та інше);

✓загрози на рівні апаратного забезпечення(загрози з точки зору технічних каналів витоку інформації).

[1]Під загрозою будемо розуміти загрозу порушення цілісності, конфіденціальності, доступності на неспростовності оброблюємої інформації.

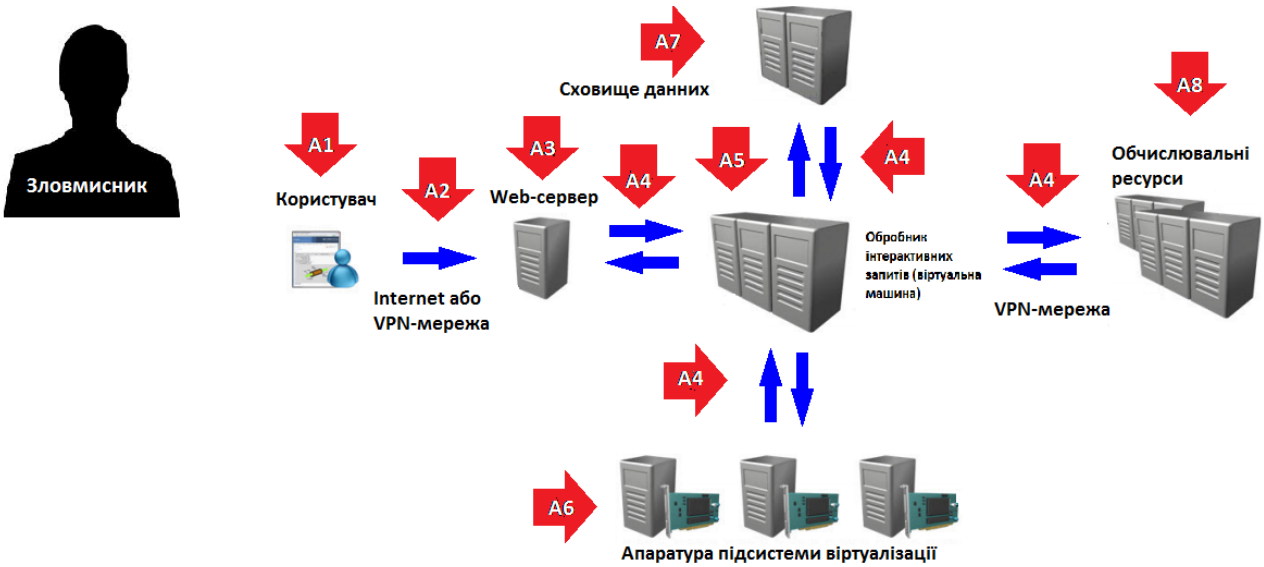

Рис. 2. Структура системи хмари з визначеними атаками

A2 – атака на рівні мережі, яка з'єднує користувача та сервер, що управляє запитами до хмари. Можливі загрози:

✓Maninthemiddle (людина всередині, тобто прослуховування та аналіз трафіка мережі без відома користувачів та системи з використанням спеціально розробленого ПЗ чи АЗ). Взагалі цей тип загрози має на увазі наступні різновиди мережевих загроз:

- видача себе за іншого користувача засобом аналізу вхідних на вихідних пакетів чи фізичне підключення до мережі;
- прослуховування трафіку як він є;
- перехоплення та навмисне переривання каналу передачі інформації.

✓Загрози пошкодження безпосередньо каналів зв'язку та їх компонентів(з технічної точки зори – кабелів, комутаторів та таке інше);

1. A3 – атака на Web-сервер, що перенаправляє запити до обробника інтерактивних запитів хмари. Можливі загрози:

✓DoSataки (перевищення кількості можливих запитів, що призводить до відмови в обслуговуванні, таким чином доступ до ресурсів хмари стає неможливим);

✓відмова апаратного обладнання (дії зловмисника чи можливі перебої електропостачання);

✓шпигунське програмне забезпечення, аналізуюче вхідні запити та відповіді.

2. A4 – атаки на рівні VPN-мережі. Можливі типи атак пов'язані лише із виходом із робочого стану пристроїв, забезпечуючих роботу мережі.

3. A-5 – атаки на обробник інтерактивних запитів хмари:

✓відмова апаратного обладнання(дії зловмисника чи можливі перебої електропостачання);

✓використання шпигунського програмного забезпечення, що може аналізувати та модифікувати вхідні та вихідні запити;

✓аналіз побічних електромагнітних випромінювань.

4. A-6,A-7,A-8 – атаки на відповідні елементи системи хмари (апаратуру підсистеми віртуалізації, сховище даних та обчислюваних ресурсів). Ці атаки можна об'єднати в один підтип атак для даної системи, бо у кожному елементі обробляється інформація, але різними засобами. Таким чином, розрізнятися будуть лише прилади, які можуть застосовуватися для аналізу та незаконного зняття інформації:

✓відмова апаратного обладнання (дії зловмисника чи можливі перебої електропостачання);

✓застосування шпигунського обладнання, що копіює чи модифікує оброблювані дані;
✓аналіз побічних електромагнітних випромінювань;
✓електротехнічні канали витоку інформації.

Таким чином, було визначено шість можливих різновидів загроз для визначеної в розд. 1 системи хмарних обчислень. За отриманими висновками можна скласти наступний графік, що виявляє вірогідності появи тієї чи іншої загрози з усіх можливих (рис.3).

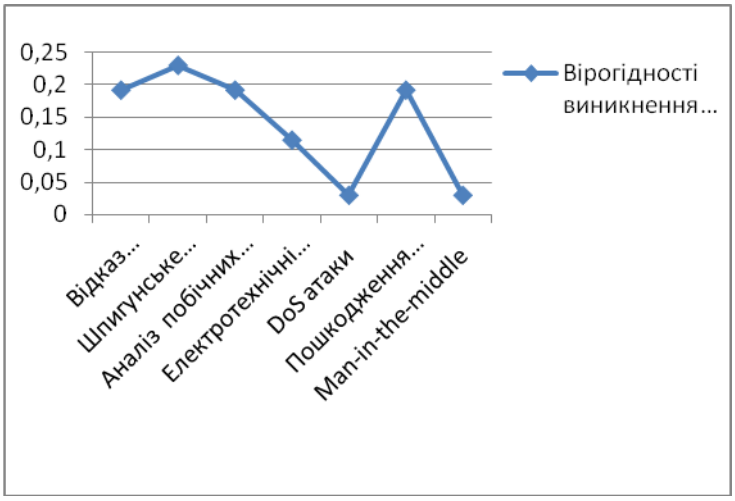

Рис. 3. Вірогідності виникнення загроз у системі хмари

З поданого графіка (рис.3) можна зробити наступні висновки: найбільш вірогідними є загрози з боку використання шпигунського програмного забезпечення. Менш вірогідними, але достатньо можливими, є такі загрози як: відмова програмного забезпечення, аналіз побічних електромагнітних випромінювань та пошкодження каналів зв'язку [5].

5. Забезпечення захисту інформації у системі хмари

На основі проведеного аналізу поданої у розд.1 системи хмари можна зробити висновок, що безпека системи в цілому складається з безпеки її окремих компонентів. Якщо розглядати систему хмари з точки зору користувача, то стає очевидним той факт, що безпосередньо під контролем користувача знаходиться тільки його персональний комп'ютер, бо сама структура хмари може бути рознесена між різними містами планети. Таким чином, для того щоб контролювати безпеку своєї інформації на певному рівні, буде доречно використовувати засоби криптографічного захисту інформації, які є найбільш надійними на даний момент. Тобто безпосередньо від користувача до мережі інформація буде поступати вже зашифрованою та з використанням певних протоколів обміну даними. Цей процес демонструє рис.4.

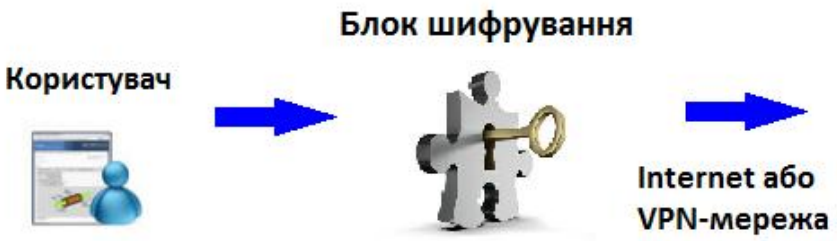

Рис. 4. Механізм подання інформації в мережу

Для шифрування користувач подає інформацію до блоку шифрування (програмне забезпечення), а вже після цього інформація певним чином потрапляє до мережі. Таким

чином, забезпечується конфіденційність інформації. Що стосується доступності, неспростовності та цілісності, далі на інформацію впливають такі фактори, які не залежать від дій користувача, тому рішення про використання тієї чи іншої мережі чи провайдера хмарних послуг треба обирати ретельно [3].

Висновки

Технологія хмарних обчислень широко використовується в останні роки у всіх сферах науки і техніки. Цьому факту сприяють переваги такого роду обчислень, що дозволяють діяти розробникам та звичайним користувачам необмежено об'ємами власних ресурсів. Це сприяє розвитку оптимальних мереж, комп'ютерів та обчислювальних пристроїв, які не повинні мати складне програмне забезпечення або великий об'єм оперативної пам'яті для виконання певних операцій.

При використанні хмарних обчислень не можна нехтувати безпекою оброблюваних даних, адже користувач не може контролювати весь процес обробки своїх даних. Перед тим, як починати використання хмарних систем, треба ретельно визначити важливість оброблюваних даних, необхідність виконання певних операцій над ними та конкретного провайдера хмарної технології, що буде використовуватися.

Необхідності забезпечувати певний рівень захисту даних сприяють деякі властивості системи хмарних обчислень, які, з одного боку, роблять технологію рентабельною та актуальною, а з іншого - надають зловмиснику можливість посягання на сторонні конфіденційні дані. Якщо головним для користувача є забезпечення конфіденційності при обчисленнях в хмарах, то найкращим засобом захисту можна назвати криптографічний захист інформації. Таким чином, для розробки системи захисту інформації будуть застосовуватися певні шифри, протоколи захищеного обміну даними, направлене шифрування та інші засоби криптографічного захисту.

При використанні шифру певної стійкості рівень або вірогідність розкриття інформації можна буде визначити відповідно, з цього випливає, що в цей момент конфіденційність інформації починає залежати лише від стійкості шифру, обраного для криптографічного захисту інформації. Це означає, що в цілому ступінь захищеності системи буде залежати від якості використаного для захисту програмного забезпечення.

У подальших роботах планується обрати, реалізувати та проаналізувати деякі протоколи захищеного обміну даними та шифри, які в перспективі можуть бути вжиті при розробці системи забезпечення конфіденційності при обчисленнях в хмарі.

Список літератури: 1. *Хмарні* обчислення та аналіз інформаційної безпеки у хмарі / І.Ф.Аулов, І.Д.Горбенко // Прикладна радіоелектроніка. – 2013. – Т. 12. – №2. – С.194-201. 2. *T.Mather, S.Kumaraswamy,S.Latif.* Cloud Security and Privacy:An Enterprise Perspectiveon Risks and Compiliance, O`ReillyMedia,2009.-334c. 3. *Електронний* ресурс: www.ibm.com/cloud-computing/us/en/ 4. *Cloud* Computing Synopsis and recommendations DRAFT,NIST,2011. 5. *The NIST* Defifnition of Cloud Computing, NIST Special Publication 800-145,2011. 6. *Guidelines* on Security and Privacy in Public Cloud Computing, NIST SP800-144,2011.

Харківський національний університет
ім. В.Н.Каразіна

Надійшла до редколегії 24.01.2014