Моделювання загроз для хмарного середовища

Мордовин О.С.
Науковий керівник – к.т.н.,доц. Чорненький В.І.
Хмельницький національний університет

Нині до хмарних технологій та реалізації на їх основі середовища хмарних обчислень (ХС) проявляється велика зацікавленість, а технологічно розвинені держави їх уже реалізували та широко застосовують. Використання технологій хмарних обчислень дозволяє досягти ряд переваг, основними з них є такі, як [1]: гнучкість, обчислювальна потужність, великий обсяг файлового сховища, різноманітність програмного забезпечення; повсякчасна можливість доступу до ресурсів в хмарі та швидке розгортання сервісів, можливість збільшення навантаження в хмарі; простота масштабування, резервування та самовідновлення; можливість управління навантаженнями та здійснення моніторингу в реальному часі тощо.

З точки зору здійснення захисту інформації також маються переваги, основними з яких є такі, як [2]:

- практична можливість централізованого керування конфігурацією, рівнем безпеки та здійснення аудиту;
- можливість динамічного масштабування ресурсів системи, резервування та аварійного відновлення при збоях;
- як правило, наявність штатних підрозділів, які повинні забезпечувати безпеку інформації при хмарних обчисленнях;
- централізоване розміщення програмного та програмно-апаратного забезпечень захисту інформації та захисту даних відповідно прийнятих політик безпеки тощо.

Політика безпеки інформації є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. Головною причиною запровадження політики безпеки зазвичай є вимога наявності такого документа від регулятора — організації, що визначає правила роботи підприємств даної галузі. У цьому випадку відсутність політики може спричинити репресивні дії щодо підприємства або навіть повне припинення його діяльності.

Крім того, певні вимоги (рекомендації) пред'являють галузеві або загальні, місцеві чи міжнародні стандарти. Зазвичай це виражається у вигляді зауважень зовнішніх аудиторів, які проводять перевірки діяльності підприємства. Відсутність політики викликає негативну оцінку, яка в свою чергу впливає на публічні показники підприємства — позиції в рейтингу, рівень надійності і т. Д.

Цікаво, що, згідно з дослідженням з безпеки, проведеного компанією Deloitte в 2006 році, підприємства, які мають формалізовані політики інформаційної безпеки, значно рідше піддаються злому. Це свідчить про те,

що наявність політики є ознакою зрілості підприємства в питаннях інформаційної безпеки.

У середовищі хмарних обчислень користувачі створюють багато динамічних віртуальних організацій, які насамперед ґрунтуються на довірі між цими організаціями.

Концепцію моделі хмарних обчислень часто розглядають двояко, деякі в ній бачать ризики для безпеки і нові «вектори загрози», але разом з тим дана система має новими можливостями для підвищення безпеки. Покращена спостережність інфраструктури, автоматизація та стандартизація - всі ці можливості підвищують рівень захищеності інформації. Наприклад, якщо використовувати заздалегідь заданий набір Qoud-інтерфейсів паралельно з централізованим управлінням ідентифікаційної інформацією, поряд з політикою управління доступом, то ми на порядок зменшуємо ризик доступу клієнтів до небажаних ресурсів. Такі заходи безпеки, як виконання обчислювальних сервісів в ізольованих доменах, використання шифрування до даних, значно підвищують збереження інформації, зменшуючи її втрати. Варто додати, що використання автоматичної ініціалізації і відновлення виконуваних образів скоротять простір для атак, дозволивши вирішувати ряд правових аспектів.

До основних недоліків хмарних технологій можна віднести [4]:

1. Залежність від підключення до мережі (необхідно мати копію вашого документа в хмарі і в локальних папках);
2. Захист персональних даних (не варто зберігати в хмарі конфіденційну інформацію);
3. Не кожне додаток дозволяє зберегти, наприклад, на флешку проміжні етапи обробки інформації;
4. Є ризик, що провайдер онлайнових сервісів одного разу не зробить резервну копію даних, і вони будуть загублені в результаті краху сервера;
5. Довіряючи свої дані онлайн-сервісу, втрачається над ними контроль.

Постійне підключення до мережі - для отримання доступу до послуг «хмари» необхідно постійне з'єднання з мережею Інтернет. Однак у наш час це не такий і великий недолік особливо з приходом технологій стільникового зв'язку 3G і 4G.

Програмне забезпечення та його кастомізація - є обмеження по ПО яке можна розгортати на «хмарах» і надавати його користувачеві. Користувач має обмеження в використовуваному ПО і іноді не має можливості налаштувати його під свої власні цілі.

Ризики часто виникають на інтерактивних вузлах між віртуальними машинами і є динамічним, непередбачуваним процесом. Уся процедура захисту даних побудована на конфіденційності, цілісності та доступності. Конфіденційність належить до так званої прихованої функції фактичних

даних або інформації і є однією із найжорсткіших вимог інформаційної безпеки. У випадку хмарних обчислень дані накопичуються в центрах обробки даних, де безпека та конфіденційність даних ще важливіші.

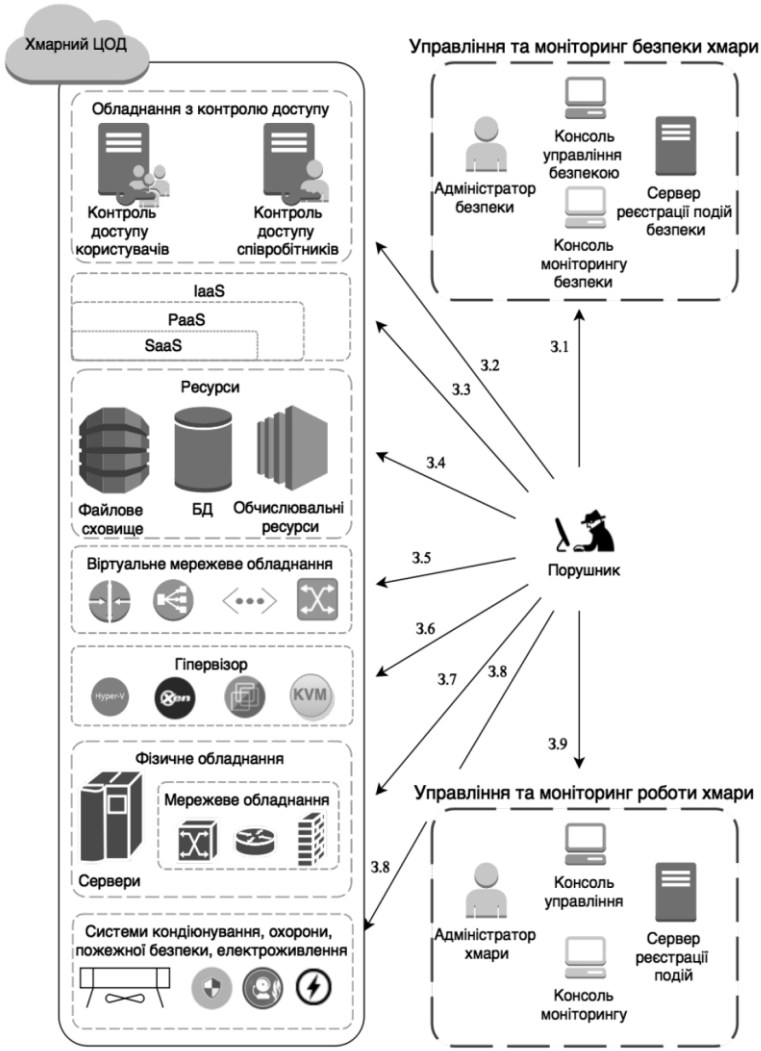

Рисунок 1– Модель загроз для хмарного середовища

Класифікація загроз за ймовірністю була проведена з урахуванням рекомендацій [5]. Згідно цих рекомендацій, найбільшу ймовірність мають загрози, що здійснюються на компоненти хмарної інфраструктури, які мають інтерфейси доступу з зовні та/або знаходяться в віртуалізованому середовищі.

Аналіз моделі загроз, зображеної на рис. 2 , показав, що найбільшу небезпеку становлять загрози управління хмарою (З.9) та її безпекою (З.1), а також загрози гіпервізору (З.6).

Модель ґрунтується на використанні поняття інформаційного віртуального з'єднання як способу опису мережевої взаємодії в ХС. Для опису привілеїв суб'єктів використовується рольова модель, в якій привілеї ролей виражені у формі правил фільтрації інформаційних сервісів для користувачів ХС. Адекватність моделі підтверджується тим, що будь-яке мережеве взаємодія в мережах TCP/IP можна представити у вигляді віртуального з'єднання, і модель включає в себе необхідні параметри для того щоб здійснити контроль мережевих з'єднань на відповідність політиці доступу.

Запропоновані на основі аналізу сучасного стану стандартизації та застосування хмарних сервісів моделі хмарних обчислень, порушника та загроз ІТС хмарних сервісів дозволили встановити, що найбільш проблемними та такими, що вимагають вирішення в частині надання послуг конфіденційності, цілісності, справжності та доступності тощо, є задачі захисту ключів та ключової інформації. Для цього на основі аналізу стану встановлено, що в середовищі хмари відносно ключових даних існують та можуть бути реалізованими такі загрози як компрометація, несанкціоноване знищення, перехоплення та запам’ятовування, нав’язування слабких та несанкціоноване використання тощо ключів. При цьому встановлено, що найбільшу небезпеку в середовищі хмарних обчислень для ключових даних користувача представляють адміністратори хмарних сервісів, які мають доступ до середовища, в якому розгорнуто хмарні додатки користувача.

Також на основі детального аналізу стану та вимог відносно безпечності управління ключами зі сторони нормативно-правових документі та стандартів, включаючи проекти, обґрунтовані механізми захисту конфіденційних, особистих та відкритих ключів користувача від виявленої множини загроз. Вони зводяться до використання для забезпечення високого рівня безпеки, тобто високого рівня ймовірностей реалізації загроз в середовищі хмарних обчислень, комплексу технічних, організаційних та організаційно-технічних заходів та засобів, в тому числі до використання:

- на рівні користувача захищених з необхідним рівнем безпеки ключових носіїв;
- на рівні каналів зв’язку між користувачем та хмарою захищених каналів зв’язку з взаємною автентифі- кацією сторін та стійкістю вищою за

стійкість ключів, що передаються;

- на рівні сервісів ідентифікації, автентифікації, авторизації та керування правами доступом надійних протоколів автентифікації з стійкими криптографічними алгоритмами, а також методів багатофакторної автентифікації;
- для здійснення криптографічних операцій на рівні сервісів додатків та інфраструктури захищених відповідним чином модулів криптографічного захисту - HSM.

Визначений в результаті аналізу перелік загроз та розроблена модель загроз ключовим даним дозволили зробити висновки про те, що порушник з високою ймовірністю може реалізовувати ряд наведених в підрозділі загроз, але найбільша небезпеку в середовищі хмарних обчислень для ключових даних користувача виникає при використанні їх в середині розгорнутою інфраструктури, без застосування криптографічних сервісів.

Перелік посилань

1. Simple Object Access Protocol (SOAP) 1.1 / World Wide Web Consortium [Електронний ресурс]. Режим доступу: http://www.w3.org /TR/2000/NOTE-SOAP-20000508/ (дата звернення 10.10.2019)

2. About Cloud Security Alliance [Електронний ресурс] / Cloud Security Alliance. Режим доступу: https://cloudsecurityalliance.org/about/ (дата звернення 10.10.2019)

3. Заборовский В.С., Сетецентрическая модель и методы контроля доступа к информационным ресурсам в среде облачных вычислений. / В.С. Заборовский, А.А. Лукашин / Научно-технические ведомости СПбГПУ. Информатика, Телекоммуникации, Управление. №2 (145) 2012. - СПб.: Изд-во Политехи. Ун-та, 2012. 183 с.

4. Зикратов, И. А. Оценка информационной безопасности в облачных вычислениях на основе байесовского подхода [Текст] / И. А. Зикратов, С. В. Одегов // Научно-технический вестник информационных технологий, механики и оптики. - 2012. - № 4 (80). - С. 121-126.

5. Hashizume, K. An analysis of security issues for cloud computing [Text] / K. Hashizume, D. Rosado, E. Fernandez-Medina, E. Fernandez // Journal of Internet Services and Application - 2013. - Vol. 4, Issue 5. - P. 15-28. doi: 10.1186/1869-0238-4-5