ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ У ХМАРНИХ СИСТЕМАХ

Назаренко Д.М.

Харківський Національний Університет
Радіоелектроніки,
Україна.

E-mail: dmytro.nazarenko1@nure.ua

Abstract

The study of protection methods in cloud systems is an important topic in the modern information technology world. Cloud systems are used to store and process large amounts of data, so security is a key aspect in their development and use. In modern cloud systems, there are various protection methods that are used to ensure the security and privacy of user data. Methods of protection in cloud systems are discussed and researched.

На сьогоднішній день нові дата-центри невизначено розмивають межі між фізичними та віртуальними середовищами, а також між публічними та приватними хмарами. Це призводить до появи багатьох питань стосовно безпеки інформації у хмарних обчисленнях. Для вирішення цих питань необхідні постійні та вдосконалені рішення [1].

Сучасні користувачі та підприємства активно використовують хмарні системи для комерційних та особистих потреб. Хоча загалом вважається, що ці системи мають надійний захист, який має запобігти будь-якій крадіжці даних, насправді хакери, використовуючи складні технології, можуть обійти ці заходи захисту. Щоб забезпечити постійну безпеку хмарних програм і сервісів зберігання даних, необхідно використовувати сучасні підходи та методи для захисту хмарних ресурсів. Такі хмарні системи повинні використовувати ті ж висококласні засоби захисту, що й традиційні автономні IT-системи.

Хмарні технології передбачають надання користувачам можливості отримувати віддалений доступ до різних послуг, обчислювальних ресурсів і програм через різні канали, зокрема Інтернет. Ця широка інфраструктура несе певні ризики та обмежує можливість контролю над її ресурсами. Точно в цьому контексті виникають актуальні питання щодо безпеки інформації та довіри користувачів до постачальників хмарних послуг.

Багато експертів попереджають про небезпеку надмірної довіри до заяв постачальників хмарних обчислень щодо безпеки [2]. Існує загальне уявлення, що користувачі хмарних послуг автоматично мають рівень захищеності у хмарному середовищі, який гарантується постачальником.

Інформаційна безпека повинна бути забезпечена на всіх етапах, включаючи постачальника хмарних рішень, користувача та їх взаємодію [3]. Користувачі хмарних послуг повинні впроваджувати власну політику безпеки, яка забороняє передачу прав доступу до інформації, яку надає постачальник, третім особам. Хмарні технології не звільняють користувачів від необхідності розробки та впровадження політики безпеки в їхніх власних системах, а також використання сервісів безпеки, які призначені для забезпечення захисту робочих місць користувачів в хмарних послуг.

У хмарних системах існують ризики інформаційної безпеки, які варто враховувати:

1. Неавторизований доступ. Можливість несанкціонованого доступу до даних або послуг у хмарних системах.
2. Втрата даних. Ризик втрати важливої інформації через технічні або людські помилки, віруси, атаки зловмисників тощо.
3. Загрози безпеки мережі. Можливість атак на мережеві з'єднання хмарних систем, які можуть призвести до перехоплення даних чи атак на конфіденційність.

4. Дотримання стандартів і регуляцій. Ризик порушення законодавства або стандартів безпеки у хмарних обчисленнях.
5. Достовірність даних. Можливість модифікації чи порушення цілісності даних під час їх збереження чи передачі через хмарні системи.
6. Слабкий захист. Недостатній рівень захисту від вірусів, шкідливих програм та інших загроз, які можуть вплинути на безпеку даних.
7. Доступність послуг. Ризик зупинки або обмеження доступності хмарних послуг через технічні проблеми або атаки на інфраструктуру хмарних систем.
Для управління цими ризиками важливо вживати відповідні заходи безпеки, включаючи шифрування даних, використання міцних паролів, регулярне оновлення програмного забезпечення та вживання інших заходів безпеки в хмарних середовищах.

У наш час є методи захисту, які використовуються у хмарних системах:
1. Шифрування даних. Для захисту конфіденційності даних, що зберігаються в хмарних системах, використовують шифрування. Дані шифруються перед відправленням до хмарного сервісу та розшифровуються лише на стороні користувача або авторизованого отримувача. Використання шифрування даних у хмарних системах має кілька ключових аспектів, включаючи конфіденційність, захист від несанкціонованого доступу, шифрування в покладенні користувача, безпеку під час передачі даних, забезпечення цілісності даних. Узагальнюючи, шифрування даних у хмарних системах відіграє ключову роль у забезпеченні безпеки і конфіденційності інформації користувачів у цьому віртуальному середовищі.
2. Аутентифікація і авторизація. Хмарні системи використовують методи аутентифікації, такі як паролі, двофакторна аутентифікація, а також механізми авторизації, щоб перевіряти і дозволяти доступ лише авторизованим користувачам. В хмарних системах, користувачі повинні успішно пройти аутентифікацію, щоб отримати доступ до хмарних послуг та ресурсів. Після аутентифікації процес авторизації визначає, до яких конкретних ресурсів чи даних користувач має доступ. Це визначається на основі прав і обмежень, які встановлені для кожного користувача або групи користувачів. Авторизація гарантує, що користувачі мають доступ лише до тих ресурсів, які їм дозволено використовувати. Таким чином, у хмарних системах аутентифікація та авторизація використовуються для забезпечення безпеки та контролю доступу до хмарних ресурсів, щоб забезпечити конфіденційність, цілісність та доступність даних для користувачів, які мають право на такий доступ.
3. Мережеві технології. Мережеві технології безпеки в хмарних системах використовуються для захисту мережі, даних та інших ресурсів в хмарному середовищі. Використання віртуальних приватних мереж (VPN) і мережевих брандмауерів допомагає захистити передачу даних між користувачем і хмарним сервісом від несанкціонованого доступу. Мережеві технології безпеки у хмарних системах мають кілька ключових аспектів, включаючи віртуальні приватні мережі (VPN), фаєрволи, інтрузії виявлення та запобігання, ідентифікація та аутентифікація, шифрування мережевого трафіку, Захист від атак на рівні мережі, мережева сегментація.
4. Моніторинг та виявлення загроз. Хмарні сервіси використовують системи моніторингу та виявлення загроз для реагування на можливі атаки, виявлення надзвичайної активності та захисту від шкідливих програм. Моніторинг та виявлення загроз у хмарних системах - це надзвичайно важливі етапи для забезпечення безпеки даних та ресурсів у віртуальних середовищах. Ці процеси у хмарних системах мають ключові аспекти, включаючи логування та аудит, використання систем інтрузійного виявлення та запобігання (IDS/IPS), аналіз поведінки, аналіз вмісту, автоматизоване виявлення загроз, реагування на інциденти, перевірка відповідності. Ці методи та технології спільно допомагають моніторити активність та вчасно реагувати на будь-які загрози у хмарних середовищах, забезпечуючи важливий рівень безпеки та захищаючи дані користувачів.
5. Резервне копіювання даних. Хмарні провайдери часто роблять резервні копії даних для запобігання втраті інформації в разі випадкового видалення або незвичайних подій, таких як кібератаки. Резервне копіювання у хмарних системах є важливою практикою для забезпечення безпеки та захисту даних користувачів. Резервне копіювання у хмарних системах має кілька ключових аспектів включаючи автоматизоване резервне копіювання, гнучкість та масштабованість, шифрування та безпека, зручний доступ та відновлення, збереження історії версій, перевірка резервних копій. Загалом, резервне копіювання у хмарних системах допомагає користувачам забезпечити безпеку своїх даних, запобігти втраті важливої інформації та відновити дані у випадку будь-яких непередбачених подій чи аварій.
6. Стандарти безпеки. Хмарні провайдери відповідають стандартам безпеки, таким як ISO 27001, що гарантує дотримання високих вимог щодо захисту інформації. Стандарти безпеки у хмарних

системах відіграють ключову роль у забезпеченні відповідності, конфіденційності та захисту даних користувачів. У наш час сучасні хмарні системи повинні відповідать найважливішим стандартам безпеки, включаючи ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, NIST SP 800-53, CSA (Cloud Security Alliance) Security Guidance, GDPR (General Data Protection Regulation). Ці стандарти надають рамки та рекомендації, які допомагають хмарним постачальникам та користувачам хмарних послуг забезпечити найвищий рівень безпеки та відповідності у своїх операціях.

7. Фізична безпека: Хмарні дата-центри зазвичай знаходяться в безпечних приміщеннях і захищені фізичними засобами безпеки, щоб запобігти фізичному доступу до обладнання. Фізична безпека у хмарних системах - це важливий аспект, який забезпечує захист фізичних компонентів і інфраструктури, які забезпечують роботу хмарних послуг. Фізична безпека у хмарних системах налічує кілька важливих аспектів, включаючи центри обробки даних (Дата-центри), захист від стихійних лих, резервні джерела енергії, теплова та вентиляційна системи, фізичний доступ до обладнання, захист від ведення війни та терористичних загроз. забезпечення фізичної безпеки у хмарних системах допомагає запобігти фізичним загрозам та зберегти надійність і доступність обслуговування хмарних послуг для користувачів.

Таким чином, перелічені методи допомагають забезпечити безпеку у хмарних системах, але важливо також звертати увагу на політику безпеки користувачів і дотримання основних правил безпеки при використанні хмарних сервісів.

*Л*ітература

1. Котяшичев И. А. Защита информации в «Облачных технологиях» как предмет национальной безопасности / И. А. Котяшичев, Е. А. Бырылова // Молодой ученый. — 2015. — №6.4. — С. 30-34..

2. The NIST Definition of Cloud Computing (англ.). [Електронний ресурс]: Режим доступа: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecia lpublication800- 145.pdf

3. Документ України щодо обробки інформації в системах хмарних обчислень [Электронный ресурс] - Режим доступа : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=58527