УДК 004.056.5 **DOI:10.30837/rt.2023.1.212.04**

М.В. ЄСІНА, канд. техн. наук, В.В. ОНОПРІЄНКО, канд. техн. наук, А.В. ТОЛОК

МОДЕЛІ ЗАГРОЗ ДЛЯ ХМАРНИХ ПОСЛУГ

Загальний огляд хмарних послуг

Хмарні сервіси – це низка IT-додатків і ресурсів, які включають програмне забезпечення, інфраструктуру та платформи, розміщені у сторонніх провайдерів і надаються на вимогу організаціям та окремим клієнтам через Інтернет. Їх також можна назвати хмарними обчисленнями.

Хмарні сервіси полегшують передачу даних на сервери постачальників послуг і з них, а також на сервери та гаджети клієнтів. Користувачі можуть отримати доступ до хмарних сервісів через комп'ютер з підключенням до Інтернету або віртуальної приватної мережі. Вони дозволяють клієнтам відмовитися від інвестицій в програмне забезпечення та придбання допоміжної мережевої інфраструктури і серверів. Використання хмарних сервісів дозволяє клієнтам отримати доступ до програмного забезпечення, хмарних сховищ, обчислювальних потужностей, IT-інфраструктури та інших послуг без необхідності нести витрати на обслуговування або оновлення програмного та апаратного забезпечення. Постачальники хмарних послуг використовують різні моделі тарифікації, які залежать від спожитих ресурсів. Зазвичай це плани з щомісячною або річною підпискою, які оплачуються за фактом використання.

Хмарні обчислення стали популярною технологією завдяки своїм численним перевагам над традиційними обчисленнями. На відміну від традиційних обчислень, хмарні обчислення дозволяють компаніям отримувати доступ до програмного забезпечення, обладнання та інших послуг віддалено, масштабуючи їх за потреби. Компанії платять лише за ті послуги, які їм потрібні, що може значно зменшити початкові інвестиції та поточні операційні витрати. Крім того, хмарні обчислення є більш безпечними та надійними, ніж традиційні, завдяки можливості віддаленого доступу до даних та високому рівню шифрування і протоколів безпеки, що використовуються постачальниками хмарних послуг.

За даними Gartner [1], традиційні IT-витрати все ще домінують над хмарними. Однак, згідно з прогнозом на 2019 – 2025 роки, витрати на хмарні технології продовжуватимуть зростати, тоді як традиційні витрати на IT продовжуватимуть скорочуватися і зрештою відставатимуть від витрат на хмарні технології з 2025 року.

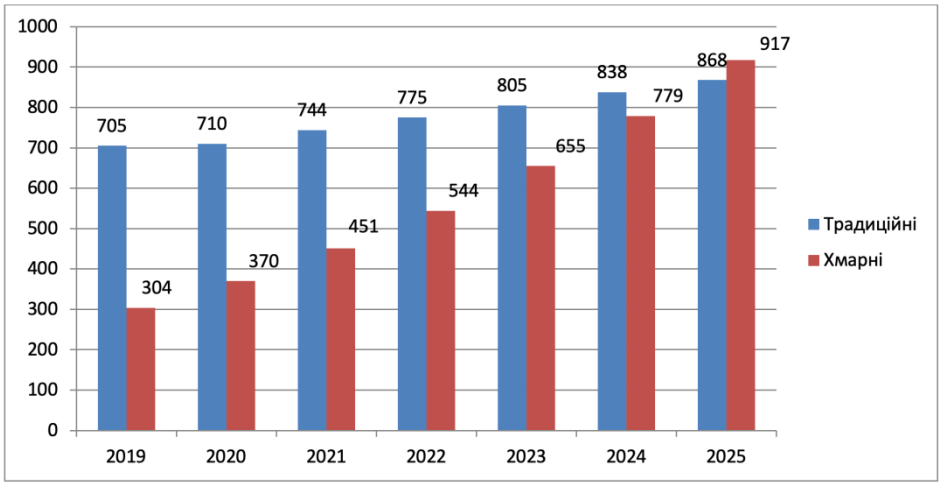

Рис. 1. Порівняння IT-витрат на традиційні та хмарні технології (млрд. $) [1]

Отже, вибір між хмарними та традиційними послугами залежить від потреб індивідуального бізнесу та його відношення до ризиків безпеки. Незалежно від того, який варіант буде

вибраний, важливо забезпечувати безпеку та захист своїх даних, використовуючи кращі практики та відповідні методики безпеки [8].

Укладаючи договір з постачальником хмарних обчислень, потрібно враховувати їх характеристики. Національний інститут стандартів США (NIST) перераховує п'ять основних характеристик хмарних обчислень: самообслуговування за запитом, широкий доступ до мережі, об'єднання ресурсів, швидка масштабованість і узгоджене обслуговування [7].

Моделі розгортання хмарних обчислень вказують на те, як хмарні сервіси стають доступними для користувачів. Існує чотири моделі розгортання, пов'язані з хмарними обчисленнями [2]:

- публічна хмара – цей тип хмарної моделі розгортання підтримує всіх користувачів, які хочуть використовувати обчислювальні ресурси, такі як апаратне (ОС, процесор, пам'ять, сховище) або програмне забезпечення (сервер додатків, база даних) на основі підписки. Найчастіше публічні хмари використовуються для розробки та тестування додатків, некритичних завдань, таких як обмін файлами та електронна пошта;
- приватна хмара – це, як правило, інфраструктура, що використовується однією організацією. Такою інфраструктурою може керувати сама організація для підтримки різних груп користувачів, або ж нею може керувати постачальник послуг, який обслуговує її на місці або за межами організації. Приватні хмари дорожчі за публічні через капітальні витрати, пов'язані з їх придбанням та обслуговуванням. Однак приватні хмари краще вирішують проблеми безпеки та конфіденційності, які сьогодні хвилюють організації;
- гібридна хмара – у цій моделі організація використовує взаємопов'язану приватну та публічну хмарну інфраструктуру. Багато організацій використовують цю модель, коли їм потрібно швидко масштабувати свою IT-інфраструктуру, наприклад, коли вони використовують публічні хмари для доповнення потужностей, доступних у приватній хмарі. Наприклад, якщо Інтернет-магазину потрібно більше обчислювальних ресурсів, він може отримати ці ресурси через публічні хмари;
- суспільна хмара – модель розгортання підтримує спільне використання обчислювальних ресурсів кількома організаціями, які є частиною спільноти. Прикладами можуть бути університети, які співпрацюють у певних галузях. Доступ до хмарного середовища спільноти зазвичай обмежується членами спільноти.

Таблиця 1

Обслуговування та управління різними видами хмарних ресурсів

Вид хмари	Ким обслуговується	Хто є власником	Де знаходиться інфраструктура	У кого є доступ
Публічна	Зовнішнім провайдером	Зовнішній провайдер	У зовнішнього провайдера	У будь-якого користувача
Приватна/ суспільна	Користувачем або зовнішнім провайдером	Користувач або зовнішній провайдер	У зовнішнього провайдера або у користувача	У авторизованого користувача
Гібридна	Користувачем і зовнішнім провайдером	Користувач і зовнішній провайдер	У зовнішнього провайдера і у користувача	У авторизованих і у будь-яких зовнішніх користувачів

Моделі обслуговування хмарних технологій

Існують три основні моделі обслуговування хмарних сервісів [5]: програмне забезпечення як послуга (SaaS), інфраструктура як послуга (IaaS) та платформа як послуга (PaaS). Моделі ціноутворення хмарних сервісів поділяються на моделі з оплатою за використання, на основі підписки та гібридні, що є поєднанням моделей з оплатою за використання та підписки.

Постачальники програмного забезпечення як послуги (SaaS) розміщують додатки, роблячи їх доступними для користувачів через Інтернет. Завдяки SaaS компаніям не потрібно встановлювати або завантажувати будь-яке програмне забезпечення в існуючу IT-інфраструктуру. Модель гарантує, що користувачі завжди використовують найновіші версії програмного забезпечення. Обслуговуванням і підтримкою займається постачальник.

Основна перевага продуктів SaaS полягає в тому, що організації можуть використовувати їх одразу після підписки, оскільки це найпростіша в налаштуванні та експлуатації хмарна модель. Щоб додати користувачів, організаціям достатньо оновити свої існуючі плани або підписки. Їм не потрібно купувати додаткове місце на сервері або ліцензії на програмне забезпечення. Основним недоліком моделі є відсутність контролю. Організації не мають контролю над хмарною інфраструктурою своїх провайдерів. Отже, якщо у провайдера трапляються перебої в роботі, то і у них теж.

Платформа як послуга (PaaS) пропонує платформу для розробки та розгортання програмного забезпечення через Інтернет, надаючи їм доступ до найсучасніших інструментів. PaaS надає фреймворк, який розробники можуть використовувати для створення індивідуальних додатків. Організація або постачальник хмарних послуг керує серверами, сховищами та мережею, а розробники керують додатками. Провайдери PaaS надають більшу частину IT-послуг для організацій, до яких користувачі можуть отримати доступ, якщо у них є підключення до Інтернету та веб-браузер. Вони також допомагають командам розробників працювати разом, незалежно від того, де вони фізично знаходяться. До недоліків можна віднести: відсутність масштабованості та прив'язку до постачальника

Інфраструктура як послуга (IaaS) використовується компаніями, які не хочуть утримувати власні дата-центри. IaaS надає віртуальні обчислювальні ресурси через Інтернет. Хмарний постачальник розміщує компоненти інфраструктури, які зазвичай існують в локальному центрі обробки даних, включаючи сервери, сховища та мережеве обладнання. IaaS полегшує, прискорює та робить більш економічно ефективним управління робочими навантаженнями для організацій, оскільки їм не потрібно купувати, управляти та підтримувати базову інфраструктуру. Хмарна інфраструктура гарантує, що компанії мають доступ до всіх необхідних ресурсів, коли вони їм потрібні. Безпека – найуразливіше місце у цій моделі. У середовищі IaaS організації передають контроль над безпекою хмари сторонньому постачальнику. Тож, навіть, якщо витік даних не вплине безпосередньо на дані компанії, скомпрометована система все одно може поставити під загрозу її діяльність. Деякі організації можуть відчувати простої в роботі з IaaS, які вони не можуть контролювати. Будь-які проблеми, що виникають у провайдера, можуть обмежити доступ компаній до додатків і даних, необхідних для щоденної роботи.

Таблиця 2

Моделі обслуговування за засобами доступу і управління

Моделі обслуговування	Засоби доступу і управління	Вміст
ПЗ як сервіс (SaaS)	Веб-браузер	Хмарні програми: соціальні мережі, офісні застосунки, системи управління вмістом, інтелектуальна обробка даних.
Платформа як сервіс (PaaS)	Хмарне середовище розробки	Хмарна платформа: мови програмування, бібліотеки, утиліти конфігурації композицій сервісів, структуровані дані.
Інфраструктура як сервіс (IaaS)	Система управління віртуальної інфраструктурою	Хмарна інфраструктура: обчислювальні сервера, сховища даних, організація мережевих з’єднань.

Загрози хмарних обчислень

Хмарна атака – це кібератака, націлена на платформи хмарних послуг, наприклад: обчислювальні служби, служби зберігання даних або програмне забезпечення. Хмарні атаки можуть мати серйозні наслідки, такі як витік даних, втрата даних, несанкціонований доступ до конфіденційної інформації та збої в роботі служб. Оскільки все більше організацій і окремих осіб покладаються на хмарні обчислення для зберігання та обробки даних, відповідно збільшується і кількість потенційних цілей для зловмисників. Найбільш значні загрози, які пов’язані з хмарними обчисленнями [3]:

– відмова в обслуговуванні (DDoS): це спроба порушити нормальну роботу системи, перевантаживши її трафіком. У випадку хмарного середовища це зазвичай відбувається шля-

хом одночасного надсилання тисяч і тисяч з'єднань. Ці запити перевантажують сервер і заважають йому обробляти законні запити;

– викрадення облікового запису: це процес, під час якого хмарний обліковий запис фізичної особи або організації викрадається зловмисником. Захоплення хмарних облікових записів є поширеною тактикою в схемах крадіжки персональних даних, коли зловмисник використовує скомпрометований обліковий запис електронної пошти або інші облікові дані, щоб видати себе за власника облікового запису;

– внутрішні загрози: це категорія ризику, яку становлять ті, хто має доступ до фізичних або цифрових активів організації. Такими інсайдерами можуть бути нинішні працівники, колишні працівники, підрядники, постачальники, які мають (або мали) санкціонований доступ до мережі та комп'ютерних систем організації;

– неправильна конфігурація хмари: неправильна конфігурація є проблемою хмарних обчислень, оскільки хмарні середовища можуть бути досить складними, а виявити та виправити помилки вручну може бути важко. Це будь-які збої, прогалини або помилки, які можуть наразити ваше середовище на ризик під час переходу на хмарні технології. Ці кіберзагрози проявляються у вигляді порушень безпеки, що можуть бути використані для несанкціонований доступу до мережі;

– шкідливі файли cookie: зараження файлами cookie в хмарних додатках означає несанкціоновану модифікацію або впровадження шкідливого вмісту в файл cookie, який є невеликим фрагментом даних, що зберігається на комп'ютері користувача. У SaaS та інших хмарних додатках файли cookie часто містять облікові дані, тому зловмисники можуть модифікувати ці файли, щоб отримати доступ до додатків;

– витік даних: це кібератака, під час якої до чутливих, конфіденційних або інших захищених даних було отримано несанкціонований доступ або вони були розголошені. Порушення даних може статися в організації будь-якого розміру, від малого бізнесу до великих корпорацій.

Системи моделювання загроз

Моделювання загроз – це процес визначення, оцінки та зменшення ризиків безпеки в додатку або системі. Використовуючи систему моделювання загроз, ви можете розподілити ресурси для протидії ймовірним загрозам, захисту життєво важливих активів і підтримки безперервності бізнесу. Існують методології та стратегії, які допоможуть зрозуміти, як ваша організація вписується в зростаючий ландшафт загроз і, що ви можете зробити для його захисту.

Існує кілька фреймворків моделювання загроз, які організації можуть використовувати для виявлення потенційних загроз безпеці та вразливостей. Ось деякі з найбільш поширених фреймворків [4, 7]:

1. STRIDE: це підхід до інтеграції на більш ранніх етапах життєвого циклу розробки програмного забезпечення. Як методологія моделювання загроз, фреймворк STRIDE використовується для створення карти додатку на основі його унікальних варіантів використання та бізнес-логіки. Таким чином, його можна використовувати для виявлення та усунення потенційних вразливостей ще до того, як буде написаний хоч один рядок коду. Також можна повертатися до фреймворку STRIDE в будь-який час, поки додаток розробляється або знаходиться у виробництві, і кожного разу, коли випускається новий код, щоб побачити, як він вплине на загальний вектор атак на додаток. Використання моделювання загроз має стати вашим першим кроком на шляху до створення мереж, систем і додатків, які будуть безпечними за своєю суттю. STRIDE – це модель загроз, яку можна використовувати як основу для забезпечення безпечного дизайну додатків [10].

2. DREAD: розшифровується як пошкодження (Damage), відтворюваність (Reproducibility), можливість експлуатації (Exploitability), постраждалі користувачі (Affected users) та можливість виявлення (Discoverability). Це модель оцінки ризиків, яка допомагає пріори-

тезувати загрози відповідно до їх потенційного впливу. DREAD найбільш підходить для малих та середніх організацій, які хочуть швидкий та простий спосіб пріоритезації загроз [9].

3. PASTA: це ризико-орієнтована методологія моделювання загроз, заснована у 2015 р. PASTA дозволяє співпрацювати між розробниками та зацікавленими сторонами бізнесу, щоб по-справжньому зрозуміти ризики, притаманні вашому додатку, ймовірність атаки та вплив на бізнес, якщо відбудеться компрометація. Модель складається з семи етапів, кожен з яких діє як будівельний блок один до одного. Такий підхід дозволяє моделі загроз бути лінійним процесом і використовувати існуючі процеси тестування безпеки у вашій організації, такі як: перегляд коду, аналіз сторонніх бібліотек, статичний аналіз і моніторинг загроз для інфраструктури додатків [7].

4. Attack Trees: дерева атак – це діаграми, які зображують атаки на систему у вигляді дерева. Корінь дерева – це мета атаки, а гілки – шляхи досягнення цієї мети. Кожна мета представляється у вигляді окремого дерева. Таким чином, в результаті аналізу загроз системі створюється набір дерев атак. Використання дерев атак для моделювання загроз є одним з найстаріших і найбільш широко застосовуваних методів. Дерева атак спочатку застосовувалися як окремий метод, а потім були об'єднані з іншими методами та фреймворками [4].

Важливо пам'ятати, що ці фреймворки мають свої переваги та недоліки, тому вибір фреймворку залежить від контексту та потреб конкретної системи.

Таблиця 3

Переваги та недоліки фреймворків

Фреймворк	Переваги	Недоліки
STRIDE	Простий та ефективний у використанні. Допомагає виявити вразливості та загрози на ранніх етапах розробки	Може бути недостатньо детальним. Не надає повного огляду системи. Важко використовувати для складних архітектур
DREAD	Допомагає визначити критичні ризики та рівень загроз, є детальним та точним, може бути використаний для оцінки зроблених вдосконалень у вирішенні загроз	Може бути складним у використанні для новачків. Недостатньо гнучкий для деяких типів систем
PASTA	Надає широкий огляд системи, включаючи аналіз атак. Допомагає знайти слабкі місця в системі. Детальний та комплексний	Використання потребує багато часу. Недостатньо гнучкий для деяких типів системи
Attack Trees	Допомагає виявляти потенційні загрози та визначати критичні елементи системи. Може бути використаний для різних типів систем. Простий та ефективний у використанні	Недостатньо детальний для деяких складних систем. Може використовувати значну кількість ресурсів для виконання

Захист від загроз хмарних послуг

Безпека хмарних послуг стає критичною проблемою, оскільки все більше компаній завершують свою цифрову трансформацію. Хмарні обчислення супроводжують новий робочий світ без кордонів, що сприяє вільному потоку інформації. Це дозволило компаніям бути більш продуктивними і зробило можливою віддалену роботу. Щоб захистити хмарні сервіси від загроз, важливо застосовувати комплексний підхід, який враховує унікальні ризики, пов'язані з хмарними середовищами. Ось кілька найкращих засобів захисту від загроз для хмарних сервісів [11]:

1. Шифрування: Шифруйте дані як у стані спокою, так і під час передачі. Переконайтеся, що ключі шифрування зберігаються належним чином.

2. Мережева безпека: Впроваджуйте засоби контролю мережевої безпеки, такі як брандмауери, системи виявлення/запобігання вторгнення.

3. Контроль доступу: Використовуйте контроль доступу на основі ролей, щоб гарантувати, що користувачі мають доступ лише до тих ресурсів, які їм потрібні.

4. Управління виправленнями: Оновлюйте все програмне забезпечення та системи найновішими оновленнями безпеки, щоб зменшити ризик їх використання зловмисниками.

5. Резервне копіювання та аварійне відновлення: Впровадьте комплексний план аварійного відновлення, щоб мінімізувати вплив будь-якої потенційної втрати даних.

6. Моніторинг загроз: Впровадьте систему моніторингу загроз для виявлення та реагування на інциденти безпеки в режимі реального часу.

Ці засоби захисту є гарною відправною точкою для організацій, щоб захистити свої хмарні сервіси від цілого ряду ризиків безпеки. Однак важливо відзначити, що безпека – це безперервний процес, і організаціям необхідно регулярно переглядати і оновлювати свої системи безпеки, щоб залишатися на крок попереду нових загроз.

Висновки

Хмарні послуги забезпечують користувачам можливість зберігання та обробки даних на віддалених серверах, що дає їм доступ до цих даних з будь-якого місця та пристрою з підключенням до Інтернету. Основною перевагою хмарних послуг є їх гнучкість, ефективність та високий рівень захисту даних.

Обираючи постачальників хмарних послуг, потрібно враховувати основні характеристики хмарних обчислень: самообслуговування за запитом, широкий доступ до мережі, об'єднання ресурсів, швидка масштабованість і узгоджене обслуговування, моделі розгортання (публічна хмара, приватна хмара) та модель обслуговування (SaaS, PaaS, IaaS). Щоб захистити хмарні сервіси, важливо використовувати комплексні підходи. Щодо моделювання загроз слід використовувати фрєймворки моделювання загроз. Важливо пам'ятати, що фреймворки мають свої переваги та недоліки, тому вибір залежить від контексту та потреб конкретної системи.

Список літератури:

1. Cloud Computing Statistics (2023). [Електронний ресурс]. Режим доступу: https://parachute.cloud/cloud-computing-statistics/.

2. Cloud Deployment Models. [Електронний ресурс]. Режим доступу: https://www.geeksforgeeks.org/cloud-deployment-models/.

3. What are Cloud Security Threats? [Електронний ресурс]. Режим доступу: https://www.vectra.ai/learning/cloud-security-threats.

4. Threat Modeling 12 Available Methods. [Електронний ресурс]. Режим доступу: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/.

5. IaaS vs. PaaS vs. SaaS: Cloud Service Model Overview [Електронний ресурс]. Режим доступу: www.intel.com/content/www/us/en/cloud-computing/as-a-service.

6. What is PASTA Threat Modeling?. [Електронний ресурс]. Режим доступу:https://versprite.com/blog/what-is-pasta-threat-modeling/.

7. Essential Cloud Computing Characteristics. [Електронний ресурс]. Режим доступу: https://www.synopsys.com/cloud/insights/essential-cloud-computing-characteristics.html.

8. Cloud Computing vs Traditional Computing. [Електронний ресурс]. Режим доступу: https://www.simplilearn.com/cloud-computing-vs-traditional-computing-article.

9. Threat Modeling with DREAD. [Електронний ресурс]. Режим доступу: https://cyral.com/glossary/threat-modeling-with-dread/.

10. STRIDE Threat Modeling: What You Need to Know. [Електронний ресурс]. Режим доступу: https://www.softwaresecured.com/stride-threat-modeling/.

11. Cloud Infrastructure Security: 7 Best Practices to Secure Your Sensitive Data. [Електронний ресурс]. Режим доступу: https://www.techtarget.com/searchsecurity/definition/cloud-security.

Надійшла до редколегії 11.02.2023

Відомості про авторів:

Єсіна Марина Віталіївна – канд. техн. наук, Харківський національний університет імені В.Н. Каразіна, доцент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; науковий співробітник-консультант АТ «Інститут Інформаційних технологій»; Україна; e-mail: m.v.yesina@karazin.ua; ORCID: https://orcid.org/0000-0002-1252-7606

Онопрієнко Віктор Васильович – канд. техн. наук, АТ «Інститут Інформаційних Технологій», Генеральний директор; Україна; e-mail: v25258@gmail.com

Толок Анатолій Вікторович – Харківський національний університет імені В. Н. Каразіна, студент кафедри безпеки інформаційних систем і технологій, факультет комп'ютерних наук; Україна; e-mail: xa12850340@student.karazin.ua