Харківський національний університет імені В.Н. Каразіна

Факультет комп'ютерних наук

Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І.І._____

« » червня 2023р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

спеціальність: 125 Кібербезпека

на тему: «Аналіз та управління ризиками хмарної безпеки»

оцінка « » Керівник к.т.н Єсіна М. В.

(прізвище та ініціали/підпис)

Голова ЕК Рецензент к.т.н. Бобух В. А.

(прізвище та ініціали/підпис)

Лемешко О.В._____ Виконавець студентка групи КБ-41

Кравченко А. А.

(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Пояснювальна записка містить 76 сторінок, 13 рисунків, 1 таблицю, 2 додатки, 67 джерел**.**

Метою дипломної роботи є дослідження хмарних сервісів, особливостей їхньої структури та галузей застосування, можливих ризиків та вразливостей систем, що засновані на хмарних обчисленнях, для різних моделей розгортання та обслуговування хмар, методів запобігання цим загрозам, а також аналіз існуючих моделей безпеки, загроз та порушника, які дозволяють покращити безпеку використаних сервісів.

Об’єктом дослідження дипломної роботи є хмарні сервіси, їхні переваги та недоліки, види та типи, а також вразливості хмарних сервісів та методи їх захисту.

Методи дослідження: методи аналізу та порівняльного аналізу щодо документації, наданої постачальниками хмарних сервісів, наукової літератури, що стосується наведеної теми.

Результатами проведеної роботи є досліджені та класифіковані ризики хмарних сервісів як для постачальника, так і для користувача хмарних послуг, а також розібрані основні загрози та атаки, що є актуальними для даного типу послуг на різних рівнях, для різних моделей обслуговування та розгортання, та методи запобігання цим загрозам та атакам. Також було проаналізовано та порівняно існуючі моделі загроз та наведено моделі порушника та загроз, що є найбільш популярними та використовуваними у даній сфері. Було досліджено найбільш популярні хмарні сервіси та зроблено порівняльний аналіз найбільш популярних хмарних провайдерів в Україні.

Ключові слова: ЗАГРОЗИ, МОДЕЛЬ БЕЗПЕКИ, МОДЕЛЬ ЗАГРОЗ, МОДЕЛІ ОБСЛУГОВУВАННЯ, МОДЕЛЬ ПОРУШНИКА, МОДЕЛІ РОЗГОРТАННЯ, РИЗИКИ, ХМАРНІ СЕРВІСИ.

ABSTRACT

The explanatory note contains 76 pages, 13 figures, 1 table, 2 appendices, 67 sources.

The purpose of the thesis is to study cloud services, features of their structure and areas of application, possible risks and vulnerabilities of cloud computing systems for different models of cloud deployment and maintenance, methods of preventing these threats, as well as analysis of existing security models, threats and intruders that can improve the security of the services used.

The object of research of the thesis is cloud services, their advantages and disadvantages, types and types, as well as vulnerabilities of cloud services and methods of their protection.

Research methods: methods of analysis and comparative analysis of the documentation provided by cloud service providers, scientific literature related to the topic.

The results of this work include the study and classification of cloud service risks for both the provider and the user of cloud services, as well as the main threats and attacks that are relevant for this type of service at different levels, for different service and deployment models, and methods of preventing these threats and attacks. Also, the existing threat models were analysed and compared, and the most popular and used threat models in this area were presented. The most popular cloud services have been studied and a comparative analysis of the most popular cloud providers in Ukraine has been made.

Keywords: ATTACKER MODEL, CLOUD SERVICES, DEPLOYMENT MODELS, RISKS, SECURITY MODEL, SERVICE MODELS, THREATS, THREAT MODEL.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ ТА СИМВОЛІВ

API – Прикладний програмний інтерфейс
APT – Сучасні постійні загрози
ASP – Постачальник послуг для додатків
DNS – Система доменних імен
DOD – Міністерство оборони США
DoS – Атака на відмову в обслуговуванні
DDoS – Розподілена атака на відмову в обслуговуванні
HTTP – Протокол передачі гіпертексту
HTTPS – Захищений протокол передачі гіпертексту
IaaS – Інфраструктура як послуга
IAM – Управління ідентифікацією та доступом
ISO – Міжнародна організація зі стандартизації
MiMA – Атака "людина посередині"
NIST – Національний інститут стандартів і технології
PaaS – Платформа як послуга
SaaS – Програмне забезпечення як послуга
SLA – Типова угода про рівень обслуговування
SP – Special Publication, спеціальна публікація
SQL – Мова структурованих запитів
TLS – Transport Layer Security, протокол захисту на транспортному рівні
UML – Уніфікована мова моделювання
ВМ – Віртуальна машина
ОС – Операційна система

ВСТУП

Якщо спитати середньостатистичну людину, чи знає вона, що є хмарним сервісом, то скоріш за все, вона відповість вам, що вона зберігає там файли та ткне в іконку iCloud чи Google Drive на екрані смартфону. І дійсно, зараз майже в кожної людини є особиста хмара в смартфоні, як-то iCloud, Google Drive, Microsoft365, що дозволяють зберігати особисті дані у віддаленому сховищі або безкоштовно (у обмеженій кількості), або за фіксовану суму, спростити передачу даних між різними пристроями, отримати доступ до своїх даних з будь-якої точки світу за наявності лише будь-якого пристрою, що має доступ до мережі, та саме доступу до мережі. Але хмарні сервіси – це не лише фотографії та спогади, це поняття, насправді, набагато ширше. Перш за все слід зазначити, що хмарні сервіси засновано на технології хмарних обчислень, та саме за допомогою цього можливо розмістити та використовувати у хмарі майже будь-що, навіть робочу базу даних з усіма працюючими комунікаціями чи операційну систему.

Хмарні обчислення, взагалі – досить загальний термін, який поєднує у особі декілька підходів та моделей з надання та управління IT сервісами, тому на практиці кожен розуміє цей термін по різному. Більшість користувачів визначає хмарні обчислення лише за однією ознакою – мережевим доступом, але хмарні обчислення це набагато більш об'ємна сутність. Якщо перефразувати ці визначення, то можна сказати, що хмарні обчислення являють собою концепцію надання IT ресурсів у вигляді послуг.

Якщо трішки подивитись на історію появлення цього, то ми виявимо, що технологія, хоч і є молодою та активно розвивається в наші часи, в основі своєї має давню як світ ідею розподілу часу – в 1990х роках ідею було висловлено американським вченим Джозефом Ліклайдером [3], що винайшов ідею Міжгалактичної мережі на основі розподілення часу [4] та активно її просував. На жаль, на той час світ не мав технічних можливостей для її реалізації, тому

першою реалізацією цієї ідеї можна вважати появу ASP (Application service provider – провайдери послуг доступу до додатків) у другій половині 1990х років, а після цього у 2000х роках через помітний зріст кількості користувачів інтернету з’явився попит на послуги, і зараз технологія лише продовжує свій розвиток. До речі, саме з тих часів до нас дійшов один з найвідоміших ASP провайдерів – Salesforce.

Хмарні сервіси зазнали різкого скачку популярності, мабуть, десь в 2019 році з початком пандемії коронавірусу, коли дуже швидко та гостро стало питання знайти консенсус між необхідністю ізолювати людей задля їхньої безпеки та продовженням життя та праці в звичайному режимі. І навіть зараз, вже в постковідні часи, вони не збавляють темпів свого розвитку. Нещодавно галузевий аналітик Gartner спрогнозував, що у 2023 році витрати кінцевих користувачів на публічні хмарні сервіси в усьому світі сягнуть майже 600 мільярдів доларів США. На жаль, через постійний розвиток та зміни, збільшення попиту використання та обсягу даних, що завантажуються в хмари, зростає ще й кількість ймовірних хакерських атак та поява інших проблем безпеки, що потрібно вирішувати для комфортного й безпечного користування сервісами. Тому актуальність вивчення безпеки хмар не визиває сумнівів – ця галузь буде лише розвиватись та розвиватись.

Метою даної дипломної роботи є дослідження та аналіз ризиків хмарної безпеки. В результаті роботи буде сформовано моделі порушника та існуючі рішення для актуальних загроз.

1 ОГЛЯД, АНАЛІЗ ТА ДОСВІД ВИКОРИСТАННЯ ХМАРНИХ СЕРВІСІВ

1.1 Загальна концепція

Згідно з визначенням Національного інституту стандартів і технології (NIST) США, хмарні обчислення (від англ. Cloud Computing) – це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), і які можуть бути оперативно надані та вивільнені з мінімальними управлінськими затратами та зверненнями до провайдера [1]. Провайдер надає ці ресурси за щомісячну абонентську плату або виставляє рахунки відповідно до використання.

NIST [1] також виділяє низку ключових особливостей цієї технології:

- Самообслуговування на вимогу. Споживач може автоматично та самостійно, не вимагаючи людської взаємодії з жодним постачальником послуг, в міру необхідності обирати та змінювати обчислювальні можливості, наприклад, серверний час і обсяг мережевого сховища.
- Широкий доступ до мережі. Весь доступ здійснюється через мережу і за допомогою стандартних механізмів, які сприяють використанню клієнтських платформ (наприклад, мобільні телефони, планшети, ноутбуки та робочі станції).
- Об'єднання ресурсів. Обчислювальні ресурси провайдера об'єднуються для обслуговування декількох споживачів за допомогою моделі з декількома орендарями, з різними фізичними та віртуальними ресурсами, що динамічно призначаються та перепризначуються відповідно до попиту споживачів. Існує відчуття незалежності від місця розташування, оскільки клієнт, як правило, не контролює і не знає точного місця розташування наданих ресурсів, але може вказати місце розташування на більш високому рівні абстракції (наприклад,

країна або центр обробки даних). Приклади ресурсів включають зберігання, обробку, пам'ять і пропускну здатність мережі.

- Швидка еластичність. Ресурси гнучко надаються та звільняються, в деяких випадках автоматично, для швидкого масштабування назовні та всередину відповідно до попиту. Для споживача можливості, доступні для надання, часто здаються необмеженими і можуть бути використані в будь-якій кількості в будь-який час.
- Вимірюваний сервіс. Хмарні системи автоматично контролюють та оптимізують використання ресурсів, використовуючи можливості вимірювання на певному рівні абстракції, що відповідає типу послуги (наприклад, зберігання, обробка, пропускна здатність та активні облікові записи користувачів). Використання ресурсів можна відстежувати, контролювати та звітувати, забезпечуючи прозорість як для постачальника, так і для споживача послуги, що використовується.

Як було зазначено вище, в людській свідомості хмарні обчислення визивають не зовсім точне уявлення про технологію, тому немає нічого дивного в тому, що цей термін має не лише одне визначення – його також відносять до технології, що забезпечує роботу хмари. Це певна форма віртуалізованої IT-інфраструктури, коли усі її складові – сервери, програмне забезпечення операційної системи, мережі та інше – абстрагуються за допомогою спеціального програмного забезпечення так, щоб їх можна було об'єднувати і розділяти незалежно від фізичних апаратних кордонів. Наприклад, так можна один апаратний сервер розділити на кілька віртуальних серверів.

Віртуалізація дозволяє хмарним провайдерам найбільш ефективно використовувати ресурси своїх дата-центрів. Саме це і є причиною того, що багато корпорацій прийняли та використовують зараз хмарну модель надання послуг для своєї локальної інфраструктури, щоб досягати максимального використання та економії коштів у порівнянні з традиційною IT-

інфраструктурою, а також пропонувати своїм кінцевим користувачам такі самі самообслуговування та гнучкість.

Якщо ж поринути трішки в історію виявлення терміну, то виявиться, що хмарні обчислення своєю назвою зобов’язані саме ознаці повсюдного мережевого доступу, незважаючи на те, що сам термін набагато ширше. Термін був запозичений у телекомунікаційних компаній, що зробили радикальне змінення від парадигми мережевого з'єднання точка-точка до віртуальних приватних мереж у 1990х роках, а там він з’явився через тогочасні схеми – раніше на схемах деяку сутність об'єктів, не істотну у даному контексті, доступ до ресурсів якої надавався по мережі позначали, як хмару. Взагалі, здається, що поява хмарних сховищ та технологій хмарних обчислень була досить передбаченою – достатньо подивитись на графік, що демонструє розвиток IT-галузі (рис. 1.1).

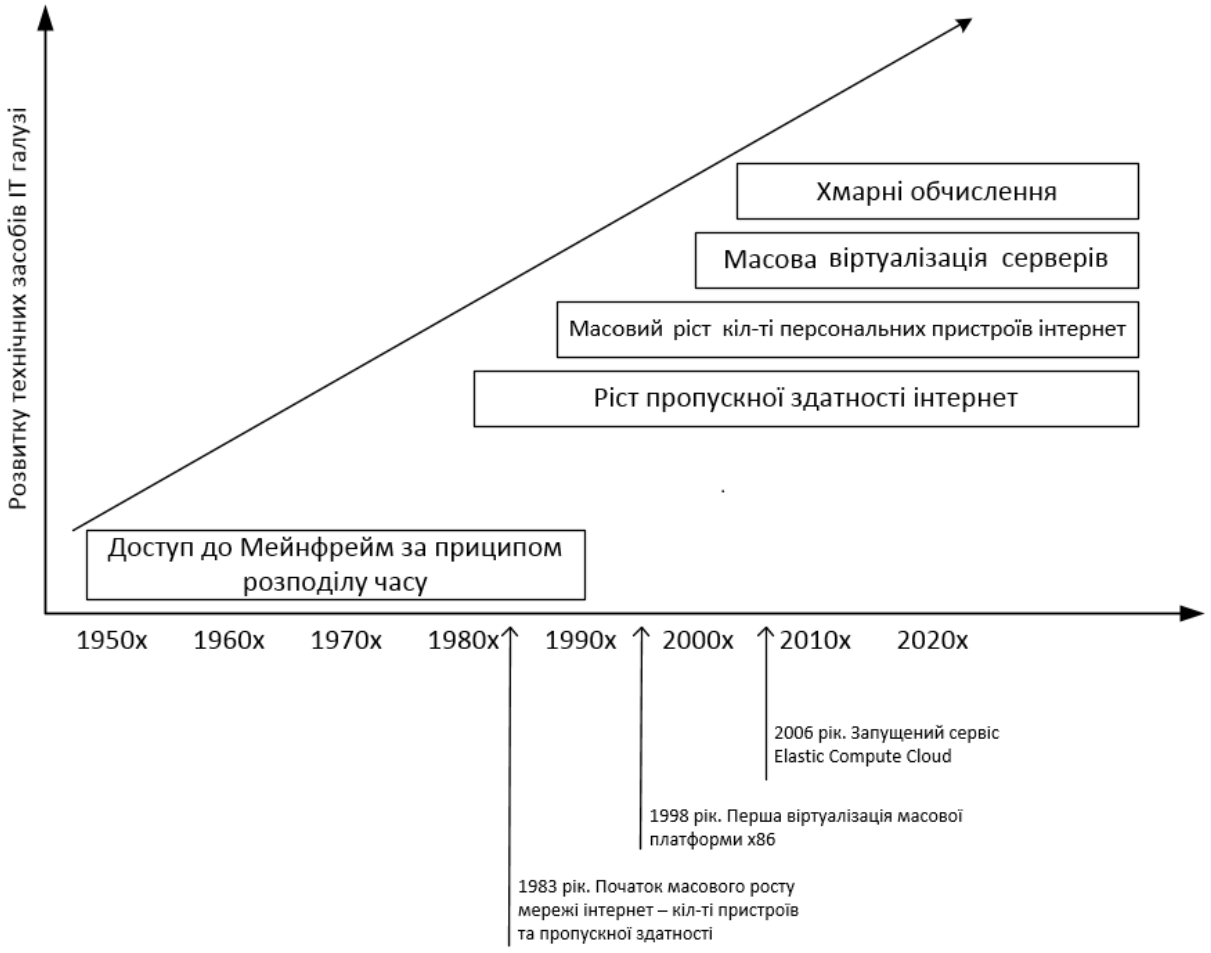

Рисунок 1.1 – Розвиток IT галузі

Взагалі, можна сказати, що хмарні обчислення являють собою концепцію надання IT ресурсів у вигляді послуг. Цей підхід є одним з наслідків більш масштабного зсуву в суспільній свідомості – переходу від продукт-орієнтованої ери виробництва до сервіс-орієнтованої ери надання послуг.

Модель хмарних обчислень складається із зовнішньої та внутрішньої частин. За допомогою зовнішньої частини користувач взаємодіє з системою, внутрішня частина є власне самою хмарою. Зовнішня частина складається з клієнтського комп'ютера або мережі комп'ютерів організації і застосунків, які використовуються для доступу до хмари. Внутрішня частина містить застосунки, комп'ютери, сервери і сховища даних, які утворюють хмару сервісів.

1.2 Моделі обслуговування

Модель обслуговування визначає рівень автоматизації IT-процесів інфраструктури та рівень послуг, що надається. Зараз майже будь-що може бути такою послугою: деякі постачальники виділяють аварійне відновлення, як послугу; резервне копіювання, як послугу; сховище, як послугу; робоче місце, як послугу. Список доволі обширний, але загалом виділяють три основні моделі надання послуг за допомогою хмари.

- Програмне забезпечення як послуга (SaaS)

Постачальники хмарного забезпечення як послуги надають користувачам готовий продукт, який запускається та керується постачальником послуг. Користувачам завдяки SaaS компаніям не потрібно встановлювати або завантажувати програмне забезпечення в існуючу IT-інфраструктуру або слідкувати за оновленнями системи чи перевіряти вільну пам'ять для цих оновлень на пристрої – постачальники програмного забезпечення як послуги розміщують додатки, роблячи їх доступними для користувачів через Інтернет. SaaS також гарантує, що користувачі завжди використовують найновіші версії програмного забезпечення. Постачальники SaaS також займаються обслуговуванням і підтримкою програмного забезпечення [5]. Серед прикладів

програмного забезпечення як послуги, що працює на основі обчислювальної хмари, є сервіси Gmail та Google docs, Microsoft Office 365, Oracle ERP/HCM Cloud, SalesForce.

Переваги використання SaaS:

- Простота доступу та використання. Основна перевага продуктів SaaS полягає в тому, що організації можуть використовувати їх одразу після підписки, це найпростіша в налаштуванні, обслуговуванні та експлуатації хмарна модель. Хмарні провайдери керують усім, тому користувачам слід лише обрати підписку та оплатити її.

- Масштабованість. Для додавання користувачів організаціям достатньо оновити свої існуючі плани або підписки. Їм не потрібно купувати додаткове місце на сервері або ліцензії на програмне забезпечення.

До недоліків використання SaaS можна віднести:

- Відсутність контролю. Простота експлуатації та налаштувань має обернену сторону – організації не мають контролю над хмарною інфраструктурою своїх провайдерів. Отже, якщо у провайдера трапляються перебої в роботі, то і у них теж.

- Проблеми з інтеграцією. Організації можуть мати проблеми з інтеграцією існуючого власного програмного забезпечення з додатками SaaS, оскільки їхні внутрішні API та структури даних можуть не інтегруватися із зовнішніми додатками.

- Платформа як послуга (PaaS)

Платформа як послуга – це модель хмарного сервісу, яка надає готове до використання середовище розробки, де розробники можуть спеціалізуватися на написанні та виконанні коду для створення індивідуальних додатків. Така модель спрощує метод розробки та розгортання додатків і є дорожчою, ніж IaaS, але дешевшою, ніж SaaS. PaaS надає фреймворк, який розробники можуть використовувати для створення індивідуальних додатків. У такій моделі організація або постачальник хмарних послуг PaaS керує серверами, сховищами

та мережею, а розробники керують додатками [5]. Це допомагає користувачам бути більш ефективними, оскільки їм не потрібно турбуватися про цілу низку проблем: закупівлю ресурсів, планування потужностей, обслуговування програмного забезпечення, виправлення або будь-яку іншу роботу, пов'язану з запуском вашого додатку. Наприклад, Google Apps надає застосунки для бізнесу в режимі онлайн, доступ до яких відбувається за допомогою Інтернет-браузера, тоді як ПЗ і дані зберігаються на серверах Google. Серед прикладів та постачальників такої системи слід зазначити AWS Elastic Beanstalk, Oracle Cloud Platform, Google App Engine, Microsoft Azure, Red Hat OpenShift

Плюси PaaS:

- Простота, зручність. Користувачі можуть отримати доступ, якщо у них є лише підключення до Інтернету та веб-браузер, оскільки провайдери PaaS надають більшу частину інфраструктури та інших IT-послуг для організацій.

- Швидша розробка. Платформи PaaS надають обчислювальну інфраструктуру та інфраструктуру зберігання даних, а також такі деталі для зручного користування, як послуги з редагування тексту, управління версіями, компіляції та тестування, що допомагає розробникам ефективно створювати нове програмне забезпечення. За допомогою PaaS також дуже зручно працювати разом та синхронно, поза залежності від того, де фізично знаходяться користувачі.

До недоліків PaaS слід віднести наступне:

- Відсутність масштабованості. Інструменти PaaS трохи жорсткіші, ніж інструменти IaaS, що може бути проблемою для організацій, масштаб попиту яких може дуже різко змінюватись протягом часу.

- Прив'язка до постачальника. Постачальники PaaS мають унікальні вимоги до конфігурації, тому організаціям та користувачам може бути складно перейти від одного постачальника до іншого, не втративши результати своєї праці або без втрат комфорту.

- Інфраструктура як послуга (IaaS)

Інфраструктура як послуга – це найбільш гнучкий тип хмарного сервісу, який дозволяє орендувати апаратне забезпечення і містить лише основні будівельні блоки для хмарних та IT-технологій. IaaS надає віртуальні обчислювальні ресурси через Інтернет. Така модель обслуговування дає повний контроль над обладнанням, на якому працює додаток (сервери, віртуальні машини, сховища, мережі та операційні системи). За своєю структурою IaaS – це майже те саме, що й традиційні IT-ресурси, з якими знайомі багато IT-відділів та розробників. Інфраструктура як послуга дуже часто використовується компаніями, які не хочуть або не мають нагальної необхідності утримувати власні дата-центри. Постачальник хмарних послуг IaaS розміщує компоненти інфраструктури, які зазвичай існують у локальному дата-центрі, включаючи сервери, сховища та мережеве обладнання, а також гіпервізор або рівень віртуалізації [5]. Найбільшими представниками постачання інфраструктури, як послуги є Amazon, Microsoft, VMWare, Rackspace та Red Hat. Хоча деякі з них пропонують більше, ніж просто інфраструктуру, їх об’єднує мета продавати базові обчислювальні ресурси.

Переваги IaaS:

- Економічна ефективність. IaaS полегшує, прискорює та робить більш економічно ефективним управління робочими навантаженнями для організацій, оскільки їм не потрібно купувати, управляти та підтримувати базову інфраструктуру.

- Масштабованість. Хмарна інфраструктура гарантує, що компанії матимуть доступ до всіх необхідних ресурсів, коли вони їм будуть потрібні, та ці ресурси не буде надано даремно.

Недоліки IaaS:

- Безпека. У середовищі IaaS організації передають контроль над безпекою хмари сторонньому постачальнику. Саме тому при наявності витока даних система може поставити під загрозу діяльність компанії, навіть якщо не було скомпроментовано дані компанії.

- Технічні проблеми. Будь-які проблеми, що виникають у провайдера, впливають на користувачів, тому вони можуть обмежити доступ компаній до додатків і даних, необхідних для щоденної роботи, а саме це є причиною того, що деякі організації можуть відчувати простої в роботі, які вони не можуть контролювати.

При обиранні потрібної моделі слід враховувати багато факторів, наприклад, кількість задач, яку повинна вирішувати використана модель, можливості компанії та її безпеку. Компаніям, що використовують SaaS, не потрібно керувати використанням даних або підтримувати свої додатки. Натомість при використанні PaaS та IaaS користувачі повинні самостійно керувати використанням даних та додатків. Постачальники SaaS і PaaS керують операційними системами організацій, а користувачі IaaS повинні самі керувати своїми операційними системами. Більш детально частини, що контролюються постачальниками, розглянуто у таблиці 1, де плюсами позначено частини системи, керовані постачальником послуг. Вільні місця показують те, що контролює споживач і, як було зазначено вище, у традиційному рішенні без віртуалізації абсолютно все контролює саме споживач.

Таблиця 1.1 – Моделі обслуговування

	Сервісний підхід		
	IaaS	PaaS	SaaS
Установка патчів і оновлень протягом життєвого циклу програм			+
Завантаження даних користувача			+
Установка складних додатків з багаторівневою архітектурою			+

Продовження таблиці 1.1 – Моделі обслуговування

Установлення патчів та оновлень протягом життєвого циклу Middleware та Runtime		+	+
Установка додаткового ПЗ, бібліотек, виконувані середовища: Java, .Net (Middleware та Runtime)		+	+
Установка патчів і оновлення в перебігу життєвого циклу ОС	+	+	+
Виділення мережевих ресурсів (Фізичні порти, VLAN, IP адресації)	+	+	+
Виділення ресурсів системи зберігання даних	+	+	+
Виділення фізичного сервера	+	+	+

1.3 Моделі розгортання

Окрім різних моделей обслуговування, існують ще й різні моделі розгортання хмар, як-то приватна, публічна, суспільна або гібридна [1]. Модель розгортання хмари визначає хмарні сервіси, які споживаються, і модель відповідальності за те, хто ними керує. Вона також визначає архітектуру хмари, масштабованість обчислювальних ресурсів, те, що користувач може змінювати, послуги, що йому надаються, і те, якою частиною збірки користувач володіє. Моделі розгортання хмари також визначають відносини між хмарною інфраструктурою та користувачами (що користувачам дозволено змінювати або впроваджувати) [7].

1.3.1 Приватна хмара

Приватна хмара (англ. private cloud) – це хмарна інфраструктура, яка призначена для використання виключно однією організацією, що включає декілька користувачів (наприклад, підрозділів). Приватна хмара може перебувати у власності, керуванні та експлуатації як самої організації, так і третьої сторони (чи деякої їх комбінації). Модель розгортання приватної хмари відрізняється від інших моделей саме цим – це виділене середовище лише для одного підприємства або організації. Апаратне забезпечення та ресурси не використовуються за межами однієї компанії, саме через це приватна хмара вважається однією з найбільш захищених структур.

Отримати приватну хмару можна від провайдера публічної хмари. Хмарний провайдер ізолює ресурси зі своєї хмари і робить їх доступними лише для однієї організації, яка не буде ділити оренду з іншими компаніями. Незалежно від того, як розміщена приватна хмара, головна перевага полягає саме в її визначенні – в тому, що ресурси надаються одній організації.

Переваги:

- Менший ризик витоку конфіденційних даних, оскільки оренда обмежується лише однією організацією; дуже обмежений доступ до даних.
- Більший контроль над резидентністю сховища і конфіденційністю даних.
- Чудова альтернатива локальним обчисленням.

Недоліки:

- Значно більш обмежений каталог пропозицій послуг, що доступні для приватної хмари.
- Ціни значно вищі, оскільки початкові витрати як для постачальника хмарних послуг, так і для споживача є вищими.

1.3.2 Суспільна хмара

Така хмарна інфраструктура надається в ексклюзивне користування певній спільноті споживачів з організацій, які мають спільні інтереси (наприклад, місія, вимоги безпеки, політики та міркування щодо відповідності). Така модель хмари може належати, управлятися та експлуатуватися однією або кількома організаціями спільноти, третьою стороною або їхньою комбінацією, і хмара може існувати як на території організації, так і поза нею. В межах цієї спільноти користувачів хмари, як правило, є група однаково зацікавлених або інвестованих споживачів. Прикладом хмари спільноти може бути хмара, яку використовують кілька різних банків чи інших організацій одного типу. Найбільша перевага спільної хмари полягає в тому, що її можна пристосувати до вимог конкретної "спільноти". Насправді, про користувачів можна навіть думати як про закриту спільноту, для якої хмара не є приватною, але поза межами спілки здається саме такою. Така хмара також вважається однією з найбільш захищених.

Переваги:

- Достатньо велика частина контролю над хмарою без необхідності самостійно володіти хмарною інфраструктурою.
- Оптимізація хмарної архітектури та ресурсів для робочих навантажень хмарних обчислень відповідно вимог спілки.

Недоліки:

- Ризики, пов'язані з багатьма орендарями. Не дивлячись на те, що хмара вважається досить захищеною ззовні, існують ризики зламу всередині, що пов’язані саме з іншими організаціями, що використовують ту саму хмару.

1.3.3 Публічна хмара

Публічна хмара (англ. public cloud) – це хмарна інфраструктура, яка призначена для вільного використання широкою публікою. Публічна хмара – географічно розподілена, глобальна, часто спільна IT-інфраструктура, з логічним поділом для безпечної багатокористувацької оренди. Найважливішим аспектом

такої хмари є той факт, що публічна хмара надає своїм користувачам можливість платити за послуги за фактом використання, а це, в свою чергу, є важливим етапом розвитку суспільства та є частиною переходу від традиційної IT-моделі, яка ґрунтується на капітальних інвестиціях, до моделі, яка ґрунтується на операційних витратах. Публічна хмара має багато переваг: легка масштабованість, висока надійність, доступність та економічна ефективність, доступ до декількох обчислювальних моделей, які не завжди доступні в інших моделях розгортання, але вважається найбільш незахищеною моделлю хмар. Публічна хмара може перебувати у власності, керуванні та експлуатації комерційних, академічних (освітніх та наукових) або державних організацій (чи будь-якої їх комбінації), та зазвичай належить так званим гіперскалерам – великим провайдерам хмарних послуг. Зазвичай доступ до публічних хмар, як і до усіх інших, здійснюється через Інтернет, при тому постачальники хмарних послуг розробляють і створюють платформи для масштабування і забезпечують логічні межі безпеки, щоб клієнти могли безпечно, самообслуговувано і повністю автоматизовано користуватися середовищами.

Переваги:

- Підтримують робочі навантаження практично будь-якого масштабу
- Простота налаштування без авансових витрат
- Великий каталог послуг
- Економічна ефективність завдяки конкурентним цінам між провайдерами публічних хмар

Недоліки:

- Спільна оренда (ризик витоку конфіденційних даних до інших орендарів, ChaosDB)
- У публічній хмарі можуть не виконуватися вимоги щодо резидентності/приватності даних

- Платіть за все, що ви використовуєте. Вартість дата-центру є менш змінною та більш фіксованою.

1.3.4 Гібридна хмара

Гібридна хмара (англ. hybrid cloud) – це хмарна інфраструктура, що складається з двох або більше різних хмарних інфраструктур (приватних, суспільних або публічних), які залишаються унікальними сутностями, але при тому з'єднані між собою стандартизованими або приватними технологіями, що уможливлюють перенос даних та прикладних програм (наприклад, використання ресурсів публічної хмари для балансування навантаження між хмарами). Гібридна модель має деякі невирішені питання безпеки саме через це поєднання, але це друга за популярністю модель. Оскільки багато компаній зробили значні інвестиції у власне обладнання і потребують його використання в процесі міграції в хмару, або через вимоги безпеки не можуть працювати в публічній хмарі, вони обирають гібридну, що також дозволяє здійснювати плавний перехід до публічної хмари протягом тривалого періоду часу та поєднати вимоги безпеки з можливостями публічної хмари. У такому випадку організації запускають критично важливі програми з конфіденційними даними локально, зберігаючи при цьому модель розгортання публічної хмари. Важливим аспектом такої моделі є пропускна здатність між хмарами, особливо в випадках, коли хмари повинні взаємодіяти в режимі реального часу.

Переваги:

- Можливість міграції з локальних на масштабовані хмарні рішення без втрати систем.
- Зменшення витрат при міграції в хмару, одночасно зменшення витрат на локальний центр обробки даних.
- Доступ до хмарних сервісів зі свого центру обробки даних.
- Збереження своїх конфіденційних даних на місці та конфіденційність, що краще контролюється.

Недоліки:

- Управління інфраструктурою є складним і трудомістким.
- Міграція між локальними та хмарними сервісами не завжди однозначна.
- Масштабування локальних систем все ще залишається складним завданням і може обмежити масштабованість вашої системи
- Через складну архітектуру складніше діагностувати та виправляти збої.

1.4 Досвід використання

Хмарні сервіси, здається, набули величезної популярності з початку епідемії коронавірусу і продовжують набирати оберти у постковідні часи. Початок пандемії став прикладом несприятливого шоку, який перевірив здатність компаній пристосовуватися до сплесків ринкової активності та переходу на віддалену роботу для співробітників. Зараз майже усі організації перейшли на використання хмарних сервісів у їх повсякденній роботі, як і дуже багато людей експлуатують хмарні сервіси у особистих цілях.

1.4.1 Найбільш розповсюджені світові хмарні сервіси

Розберемо 4 найбільш відомих та використовуваних у світі хмарних сервісів та їх можливості за версією Gigacloud Ua – лідера серед постачальників послуг в Україні [8, 9].

Google One (Диск) – це хмарний додаток для зберігання, редагування та синхронізації файлів, розроблений компанією Google [10].

Можливості:

- Можна зберігати файли будь-якого формату: фото, відео, аудіо. У кожному акаунті Google безкоштовно доступно 15 ГБ пам'яті.
- Відсутня прив'язка до конкретної операційної системи.
- Файли на диску можна відкривати зі смартфона, планшета або комп'ютера.

- Для поширення файлів треба лише змінити права доступу до нього у пару кліків.

Microsoft Office 365 – це хмарний сервіс, який поєднує зручні сучасні інструменти для роботи, що поширюються на основі передплати [11]. У пакет Microsoft Office 365 входить:

- Електронна пошта бізнес-класу на сервері Exchange.
- Портал Sharepoint і публічний сайт-візитка з простим конструктором сторінок.
- Комунікатор Lync, за допомогою якого можна обмінюватися текстовими фразами, проводити відео- та аудіоконференції, здійснювати показ робочого столу.
- Доступ до додатків останньої версії Microsoft Office.
- Доступ до додатків Microsoft Office 2010, 2013 і 2016 корпоративному тарифному плані.
- Місце в OneDrive (1 терабайт на користувача).

Serpstat – це багатофункціональна SEO-платформа, яка дозволяє проводити моніторинг позицій, аналіз зворотних посилань, робити SEO-аудит сайту, аналізувати семантику і аналітику конкурентів [12].

Можливості:

- Порівнює дані сайтів зі схожою тематикою.
- Збирає дані про конкурентів в органічній видачі та в контекстній рекламі.
- Показує тексти оголошень конкурентів.
- Аналізує середній бюджет конкурентів на рекламу.
- Перевіряє релевантність URL семантиці сайту і багато іншого.

Deals – онлайн-сервіс підписання документів електронним підписом. Сервіс допомагає оперативно приймати рішення, знижує витрати на процеси документообігу між керівником, бухгалтером, фінансистом, IT-фахівцем і юристом [13].

Переваги:

- Збільшує кількість узгоджених вчасно документів.
- Скорочує тривалість підготовки та узгодження документів.
- Прибирає витрати на доставку і обмін паперовими документами між контрагентами.
- Надає цілодобовий доступ до документів.

1.4.2 Аналіз постачальників хмарних сервісів в Україні

На жаль, окрім загальносвітової проблеми і актуальності віртуалізації, пов'язаною з пандемією, в нашій країні виникла інша, не менш гостра причина для багатьох компаній збільшити користування хмарними сервісами. У зв'язку з початком повномасштабного вторгнення росії більшість IT-компаній з офісами на сході України зіткнулися з необхідністю переміщення співробітників в інші регіони, а також організації робочого процесу віддалено, для чого необхідний доступ до хмарних сервісів [8].

Згідно дослідженню дослідницької компанії Molfar [14], серед лідерів надання хмарних послуг в Україні перше місце поділили GigaCloud та Tetcloud. Порівняння відбувалось за такими критеріями: реакція та умови комерційної пропозиції, термін її підписання, забезпечення технічної сторони питання – тестування відбувалось на надання інфраструктури, як послуги серед компаній-постачальників такої моделі обслуговування (рис. 1.2).

GigaCloud отримали найбільшу кількість балів у категорії «Реакція та умови КП». Tetcloud отримали найвищі оцінки за роботу техпідтримки у категоріях «Підписання договору» та «Технічна частина». Друге місце розділили De Novo та Tucha також отримавши високі бали у категоріях «Реакція та умови КП» та «Технічна частина». Третє місце посіли Парковий, здобувши високі бали за роботу технічної підтримки у всіх трьох категоріях. Серед аутсайдерів же опинились DataGroup та Adamant [15].

Компанія	Місце 2021	Δ, %	Місце 2022
GigaCloud	1	-	1
Tetcloud	4	+3 ↑	1
Tucha	3	+1 ↑	2
Парковый	2	- 1 ↓	3
SIM-Networks	-	-	5
DE-Novo	2	-	2
DataStore	4	-	4
United-DC	7	-	7
Vodafone	-	-	6
U-Cloud	4	- 2 ↓	6
Cosmonova	6	- 4 ↓	10
Colocall	-	-	9
Volia	-	-	8
DataGroup	-	-	11
Adamant	-	-	12

Рисунок 1.2 – Результат у вигляді рейтингової таблиці в порівнянні 2022 з 2021 роком

2 АНАЛІЗ РИЗИКІВ ХМАРНИХ СЕРВІСІВ

Хмарні сервіси, не дивлячись на те, що постачальники послуг постійно вдосконалюють їхні системи безпеки, складно назвати зовсім захищеними: дані, що зберігаються та обробляються, можуть бути скомпроментовані, втрачені або пошкоджені. Додатково ускладнює ситуацію саме використання технології віртуалізації, що є основною для технології хмарних обчислень. Звісно, набагато простіше захистити від небезпеки те, що зберігається на комп'ютері, ніж десь на віддаленому сервері. У цьому розділі наведено основні загрози та ризики для хмарних сервісів. Взагалі, для хмарних сервісів загрози безпеки є основною проблемою, тому необхідно класифікувати ризики, які можуть перешкоджати ефективності бізнес-процесів, розгорнутих у хмарі. Існує класифікація, що називається таксономією ризиків безпеки хмарних обчислень. Таксономія ризиків безпеки хмарних обчислень поділяє ризики на шість категорій – це безпека даних, логічний доступ, мережева безпека, фізична безпека, відповідність вимогам і віртуалізація, як показано на рисунку 2.1 [16].

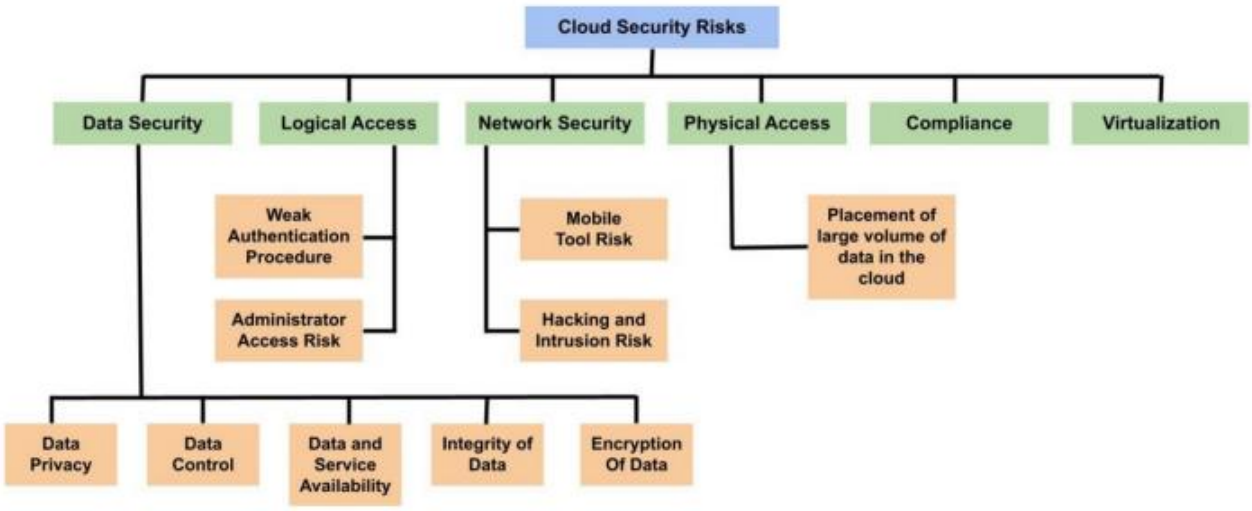

Рисунок 2.1 – Таксономія ризиків безпеки

2.1 Безпека даних

Ризики безпеки даних є основною перешкодою для хмарних обчислень. Багато людей та організацій не користується хмарами тому, що вони не довіряють свої конфіденційні дані хмарам саме через можливий витік довірених даних. В свою чергу, ризик безпеки даних теж можна поділити на декілька умовних груп: ризики, що стосуються контролю даних; конфіденційності, цілісності та доступності даних, шифрування даних тощо.

2.1.1 Контроль даних

Хмарний провайдер управляє даними, розміщеними в хмарі, і тому вони знаходяться поза контролем організації [17]. Інфраструктура захисту даних є спільною для багатьох споживачів, місцезнаходження даних не розкривається споживачам, оскільки дані можуть зберігатися в різних місцях у хмарі. Крім того, дані знаходяться поза межами обмеженого середовища споживачів, що призводить до витоку даних, а отже, до ризиків конфіденційності через несанкціонований доступ. Оскільки хмарні сервіси надаються у спільне користування багатьом споживачам, порушення закону організацією може призвести до вилучення всіх даних, якими керують хмарні провайдери [18].

2.1.2 Конфіденційність даних

Конфіденційність даних – це процес захисту даних від незаконного доступу та розголошення з боку аутсорсингового сервера та неавторизованих користувачів. Конфіденційність зазвичай тісно пов’язана з автентифікацією користувачів та належними методами шифрування. Це досягається шляхом шифрування даних таким чином, щоб тільки авторизовані користувачі могли їх розшифрувати. Загрози конфіденційності можна також поділити на три категорії: загрози з боку внутрішніх користувачів, зовнішні загрози та витік даних.

Перша категорія є, мабуть, найбільш поширеною, бо кожна з моделей надання послуг може спричинити потребу в декількох внутрішніх користувачах, а людська доброчесність, на жаль, не завжди є контрольованою. До неї відносять такі ризики, як загроза з боку зловмисного хмарного провайдера або зловмисного користувача хмарного сервісу.

Яскравими прикладами зовнішніх загроз можна назвати віддалені програмні атаки на хмарну інфраструктуру або хмарні додатки, або на саму хмару, або віддалені програмні та апаратні атака на кінцеві точки організацій-користувачів хмари. На жаль, всі типи моделей надання хмарних послуг схильні до впливу зовнішніх зловмисників. Але найбільше це торкається хмарних провайдерів, що зберігають та оформляють великі обсяги даних, як, наприклад, дані кредитних карток, особисту інформацію та конфіденційну державну або інтелектуальну власність.

Третя категорія – витік даних – зазвичай має на увазі порушення конфіденційності, що відбувається ненавмисно з боку користувачів або провайдерів, а через неідеальність системи. Наприклад, через збій прав доступу до безпеки в декількох доменах або збій електронних і фізичних систем транспортування хмарних даних і резервних копій. Така загроза широкомасштабного витоку даних між багатьма, потенційно конкуруючими організаціями, які використовують одного і того ж хмарного провайдера, може бути викликана людським фактором або несправним обладнанням, що призведе до компрометації інформації.

2.1.3 Цілісність даних

Доступ до даних декількох споживачів та модифікація даних хмарними провайдерами з віддалених місць може загрожувати цілісності даних [18]. Загалом, цілісність даних визначається як захист даних від несанкціонованого видалення, модифікації чи фальсифікації [19].

Цілісність даних у складних середовищах хмарного хостингу, таких як SaaS, налаштованих на спільне використання обчислювальних ресурсів між клієнтами, може становити загрозу для цілісності даних, якщо системні ресурси не будуть ефективно розділені. Тому загрозу можуть становити неправильно визначені параметри безпеки або неправильна конфігурація віртуальних машин і гіпервізорів. До помилок, що можуть призвести до загроз цілісності, також можна віднести неправильне розподілення доступу або недостатньо добре забезпечену автентифікацію даних.

Однак, окрім таких помилок, ще існує цілий ряд атак, що загрожують цілісності [20].

2.1.4 Доступність даних і послуг

Доступність даних і послуг пов'язана з відновленням даних під час порушення роботи системи для забезпечення безперебійної передачі хмарних сервісів. У випадку витоку даних після того, як конфіденційність буде порушена, процес резервного копіювання та відновлення може здатися складним. Крім того, залежність від Інтернету як засобу передачі даних може становити ризик доступності через зниження швидкості пропускної здатності каналу зв'язку [30]. Тож, серед поширених загроз доступності слід зазначити або технічні причини відсутності доступу, або хакерські атаки – наприклад, атаку відмови в обслуговуванні, зміни інфраструктури під впливом хмарних провайдерів, клієнтів і сторонніх систем, що впливають на хмарних клієнтів та атаку на систему доменних імен (DNS).

2.1.5 Шифрування даних

Відсутність належного шифрування та управління ключами даних може призвести до серйозного ризику, оскільки хмарне середовище є спільним для багатьох споживачів і хмарних провайдерів, які можуть легко отримати доступ до даних через загальнодоступну мережу. Шифрування є найпоширенішим

методом захисту усюди, та існує багато різних алгоритмів різної стійкості, та постійно виникають нові, тому слід використовувати найбільш стійкі та не скомпрометовані.

2.2 Логічний доступ

Управління доступом – один з найпоширеніших ризиків безпеки хмарних обчислень. Точка доступу – це ключ до всього, саме тому хакери так націлені на неї.

У 2016 році LinkedIn зазнав масового витоку даних користувачів, включаючи облікові дані акаунтів (приблизно 164 мільйони) [30] саме через не дуже вдалу систему розподілення логічного доступу. Або можна згадати приклад новіше – витік інформації з Пентагону, який наробив багато шуму та відбувся у лютому 2023 року, але розголосу набув лише у квітні, причиною якого стала проблема у управлінні доступом та порушення правила найменших привілей, в результаті чого люди, що не мали мати права доступу до конфіденційної інформації людям, мали його.

Зазвичай причинами успіху такої атаки є недостатній антикризовий менеджмент, неефективна інформаційна кампанія та розумність та гнучкість хакерів та використовуваних ними систем, і навіть якщо люди не можуть вплинути на останню складову, завжди можна слідкувати за першими двома. Крім того, доступ до даних через Інтернет призводить до більшої вразливості, ніж фізичний доступ до даних, що незмінно призводить до підвищення ризиків. Ризики такого доступу розглядаються нижче:

2.2.1 Ризик доступу адміністратора

Завдяки інтерфейсу управління (самообслуговування на вимогу), який вимагається хмарними обчисленнями для своїх послуг, недоброчесні адміністратори хмарних обчислень можуть легко отримувати доступ до чутливих даних і змінювати їх через Інтернет.

2.2.2 Слабка процедура автентифікації

Відсутність надійної процедури автентифікації може призвести до несанкціонованого доступу до конфіденційних даних і додатків, до яких багато споживачів можуть отримати доступ з будь-якого місця через багаторазову оренду хмарного середовища [31].

2.3 Мережева безпека

Цей пункт пов’язаний з можливістю зловмисників отримати доступ до інформації, що передається або зберігається, за допомогою віддалених систем. Окрім очевидних проблем з порушенням безпеки даних, можуть бути використані інфіковані/зловмисні програми, що можуть негативно вплинути на користувачів хмарних сервісів і хмарних обчислень. Ризики мережевої безпеки включають наступне:

2.3.1 Ризик злому та вторгнення

Хакери можуть отримати доступ до даних і додатків через віддалену систему та веб-додатки шляхом запуску інфікованих додатків, що вплине на споживачів хмарних послуг та їхні сервіси. Зазвичай таке трапляється через недостатню стійкість протоколів шифрування даних.

2.3.2 Ризик мобільних інструментів

Зараз отримати доступ до будь-якого серверу можна зі звичайного смартфону, який ми використовуємо майже завжди. Смартфони містять багато конфіденційної інформації, і люди зазвичай мало слідкують за безпекою всередині мобільних пристроїв. Цей привілей – дозвіл користувачам хмарних сервісів отримувати доступ до даних через мобільні пристрої, є новим тенденційним ризиком у хмарному середовищі, що призводить до загроз безпеці в цій сфері.

2.4 Фізичний доступ

Хмарні обчислення революціонізують світ бізнесу завдяки зручним сервісам хмарного зберігання та управління хмарними ресурсами, їх поява та шалене збільшення популярності, їхні значні переваги змусили багато організацій розмістити свої конфіденційні дані в хмарі, не замислюючись про наслідки. Розміщення великого обсягу даних у хмарі збільшує ризик зламу з боку зловмисників – захистити віддалений сервер все-ж таки складніше, ніж захищене фізичне розташування [18].

Постачальник хмарних послуг може володіти хмарним сервером, але не мати фізичного доступу до нього, тобто, не мати змоги фізично його контролювати. Щоб уникнути цього ризику, слід регулярно проводити сканування хмарної безпеки для виявлення потенційних загроз або вразливостей і вживати превентивні заходи. Хмарні провайдери також повинні надавати безпечні протоколи шифрування для спільного доступу до даних і використовувати різні методи автентифікації, щоб гарантувати, що доступ мають лише легітимні користувачі.

2.5 Відповідність вимогам

Використання хмарних сервісів, як було зазначено вище, пов'язане з віддаленим зовнішнім розташуванням бізнес-даних і додатків, які не підпадають під дію політик і регуляторних органів, що контролюють дані, які зберігаються у фізичному середовищі. Комплаєнс-ризик – це потенційна схильність організації до юридичних санкцій, фінансових втрат і матеріальних збитків, що виникають через її нездатність діяти відповідно до галузевих законів і нормативних актів, внутрішніх політик або встановлених найкращих практик.

На комплаєнс-ризик наражаються організації всіх типів і розмірів, незалежно від того, чи є вони державними або приватними, комерційними або некомерційними, державними або федеральними. Недотримання організацією

чинних законів і нормативних актів може вплинути на її доходи, що може призвести до втрати репутації, бізнес-можливостей і оцінки.

Існує декілька типів ризиків, пов’язаних з відповідністю вимогам у хмарних технологіях [32]:

- Корупційні та незаконні дії.

Дотриманість вимог гарантує, що організація, її агенти та працівники дотримуються законів і правил галузі. Загальні ризики пов'язані з незаконними практиками і включають шахрайство, крадіжки, хабарництво, відмивання грошей і розкрадання.

- Порушення конфіденційності.

Другим за поширенням ризиком такого типу є порушення законів про конфіденційність. Якщо компанія працює з конфіденційною інформацією, вона зобов'язана вживати відповідних заходів для захисту цих даних і запобігання порушенням конфіденційності. Хакерство, віруси та шкідливе програмне забезпечення – ось деякі з кіберризиків, які впливають на організації.

- Технологічні ризики.

Процесний ризик – це недотримання встановленої процедури виконання завдання або відхилення від стандартного процесу. Наприклад, компанія повинна мати задокументовану процедуру віддаленого доступу до мережі. Якщо співробітник зловживає належною процедурою віддаленого доступу, це вважається процесним ризиком.

2.6 Віртуалізація

Віртуальні ресурси неможливо відокремити від хмарних обчислень, оскільки це основа, на якій базується їх робота. Оскільки віртуальні ресурси пов'язані з хмарними засобами, ризики вторгнення стають першочерговими як один із значних ризиків безпеки в хмарному середовищі.

Згідно з Cloud Security Alliance [33], можна виділити такі ризикі, пов’язані з віртуалізацією:

- Розповзання віртуальних машин (ВМ)

Зважаючи на простоту створення віртуальних машин, застарілі та неоновлені сервери можуть поширюватися в середовищі, а конфіденційні дані можуть бути скомпроментовані.

- Безпека автономних і неактивних, попередньо налаштованих ВМ

Чим довше ВМ перебуває в автономному режимі, тим більше вона відхиляється від безпечної базової лінії. Якщо її запустити, це може становити значний ризик для зловмисників. Оскільки ВМ – це просто файли на платформі, несанкціонований доступ до них можливий, якщо немає належного захисту, тому виникає необхідність слідкувати за запущеними ВМ.

- Відсутність видимості та контролю над віртуальними мережами

Трафік, що рухається у віртуальних мережах, може бути невидимим для традиційних засобів захисту.

- Виснаження ресурсів

Багато віртуальних середовищ мають надмірні ресурси, особливо якщо всі пристрої, що працюють, використовують свої максимальні конфігурації обчислювальних ресурсів або пам'яті. Такі конфігурації можуть призвести до значного зниження продуктивності. Це часто трапляється, коли гіпервізор скомпрометовано і змінено конфігурацію сервера.

- Безпека гіпервізора

Гіпервізор – це програмне забезпечення, яке керує віртуальними пристроями в середовищі. Навіть захищений пристрій або сервер можна змінити на цьому рівні, тому його можна вважати єдиною та головною точкою відмови. Несанкціонований доступ до гіпервізора може статися через зміну операційної процедури або доступу до фізичних машин або навіть віртуальних серверів, а результатом може стати, наприклад, виснаження ресурсів, описане вище.

- Робочі навантаження з різними рівнями довіри на одному сервері

Різні робочі навантаження повинні працювати в різних віртуальних середовищах (наприклад, різне фізичне обладнання, на якому працюють

віртуальні пристрої). Для уникнення цього ризику можна відокремити розробку/тестування від виробничих віртуальних машин або додатки з конфіденційними даними від тих, що не містять таких даних.

- Ризик через API постачальника хмарних послуг

Багато організацій використовують хмарні сервіси як для SaaS, так і для IaaS, а також власне кероване віртуальне середовище. API, що використовуються для зв'язку між середовищами, можуть становити значний ризик.

Узагальнюючи усі наведені вище загрози, можна сказати, що основною і головною проблемою хмарних сервісів є витік даних. При тому, він може відбутись як від технічних проблем, що є маловірогідним, або, що є більш розповсюдженим – від дій зловмисників. Не треба також забувати про можливі вразливості самої системи хмарних сервісів – несанкціонований доступ до конфіденційних даних через Інтернет через інтерфейс самообслуговування на вимогу та слабку процедуру автентифікації в хмарному середовищі також не є вигаданою проблемою. Якщо ж ми згадуємо про хакерів, то слід також зазначити їх основні інструменти – шкідливе програмне забезпечення [33], вторгнення в публічні мережі [35], фішинг [36], використання можливих слабких місць систем за допомогою різних атак, що порушують конфіденційність, цілісність, доступність хмарних сервісів та інформації, що там зберігається. Деякі з найбільш поширених перераховано нижче [20]:

- SQL-ін'єкції

SQL-ін’єкції націлені на SQL-сервери, які запускають уразливі програми баз даних. Хакери використовують вразливі місця веб-серверів і вводять шкідливий код, щоб обійти вхід і отримати несанкціонований доступ до серверних баз даних [21].

- Атака "людина посередині" (MiMA)

MIMA зазвичай виникає, коли різні користувачі хмари спілкуються один з одним або спільно використовують ресурси з хмарного середовища [22].

Недостатнє шифрування може зробити користувачів вразливими до атаки "людина посередині", яка є непрямою атакою [23].

- Атака підробки тегів

Ця атака відбувається, якщо нечемний продавець обманює своїх клієнтів, показуючи неправильний штрих-код чи даючи неправильне посилання. Якщо користувач сканує його на своєму пристрої, то зловмисник отримує доступ до всіх конфіденційних даних, що призводить до можливих ризиків шахрайства та витоку приватної інформації [24].

- Візантійська атака

Ця атака відбувається на різні частини хмарних обчислень шляхом зупинки або виходу з ладу систем, і її результатом стає некоректне проходження запиту через систему [25].

- Сніфферні атаки

Атака відбувається коли користувач натискає на шкідливі посилання. Після того, як натиснуте посилання буде активоване, програма перехоплює потік пакетів в мережі і отримує доступ до персональних даних користувачів, таких як паролі, реквізити банківських рахунків тощо, які не є зашифрованими [28]. Залежно від обсягу даних та їх характеру, внаслідок цієї атаки втрати даних можуть бути непомітними або стати причиною великих проблем для цілої організації.

- Атака на систему доменних імен (DNS)

Причиною такої атаки є шкідливе ПЗ. DNS перетворює доменні імена на IP-адреси, і користувач не може бачити, наскільки правильно відбувається перетворення. Кожного разу, коли відкривається невідома веб-сторінка, зловмисник може легко отримати доступ до персональної інформації, що використовується на серверах [26].

- DDoS-атака

Мабуть, у сучасних технологіях це є найбільш серйозною проблемою, оскільки не може бути усуненою повністю. На сьогоднішній момент є лише деякі

методи пом’якшення наслідків, які допомагають зменшити ризики та послідовності таких атак. DDoS-атаки націлені на веб-сайти та сервери, порушуючи роботу мережевих сервісів з метою виснаження ресурсів програми. Зловмисники, які стоять за цими атаками, наводнюють сайт несанкціонованим трафіком, що призводить до погіршення функціональності сайту або взагалі виводить його з ладу [24].

- Отруєння файлами cookie

Отруєння 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 веб-сайтом або веб-додатком.

Файли cookie використовуються для зберігання інформації про вподобання користувача та історію переглядів, а також часто застосовуються для персоналізації досвіду користувача або для відстеження його активності. У SaaS та інших хмарних додатках файли cookie часто містять облікові дані, тому зловмисники можуть отруїти файли cookie, щоб отримати доступ до додатків.

- Атаки на побічний канал

Атака побічного каналу організовується хакерами, коли вони розміщують шкідливу віртуальну машину на тому ж хості, що й цільова віртуальна машина. Під час атаки побічного каналу хакери атакують системні реалізації криптографічних алгоритмів. Однак цього типу загроз можна уникнути за допомогою безпечного дизайну системи.

- Атаки "людина в хмарі"

Під час цього типу атак хакери перехоплюють і переналаштовують хмарні сервіси, використовуючи вразливості в системі токенів синхронізації, щоб під час наступної синхронізації з хмарою токен синхронізації був замінений на новий, який надає зловмисникам доступ до акаунтів. Ця атака може бути дуже непомітною – користувач може, не здогадуючись про злам, втратити акаунт назавжди.

- Сучасні постійні загрози (APT)

APT – це атаки, які дозволяють хакерам безперервно викрадати конфіденційні дані, що зберігаються в хмарі, або експлуатувати хмарні сервіси непомітно для законних користувачів. Тривалість цих атак дозволяє хакерам адаптуватися до заходів безпеки, спрямованих проти них. Після встановлення несанкціонованого доступу хакери можуть переміщатися мережами центрів обробки даних і використовувати мережевий трафік для своєї зловмисної діяльності.

- Spectre та Meltdown [37]

Ці два типи кібератак з'явилися на початку цього року і вже стали новою загрозою для хмарних обчислень. За допомогою шкідливого JavaScript-коду зловмисники можуть зчитувати зашифровані дані з пам'яті, використовуючи слабкі місця в конструкції більшості сучасних процесорів. І Spectre, і Meltdown порушують ізоляцію між додатками та операційною системою, дозволяючи зловмисникам зчитувати інформацію з ядра. Це справжній головний біль для хмарних розробників, оскільки не всі користувачі хмарних сервісів встановлюють найновіші патчі безпеки.

3 ДОСЛІДЖЕННЯ УПРАВЛІННЯ РИЗИКАМИ ХМАРНОЇ БЕЗПЕКИ

Звісно, після дослідження та аналізу усіх вразливостей та ризиків хмарних сервісів виникають питання доцільності їх використання – чи потрібні вони в такому обсязі, в якому вони існують та використовуються. Зрозуміло, що технології хмарних обчислень потребують своїх систем безпеки для існуючих для них ризиків, тому існує очевидна потреба в ефективному плані та моделях управління ризиками для захисту основних інформаційних активів [37]. Існує багато різних методів, що спрямовано на рішення якихось окремих проблем хмарних технологій – застосування надійних методів автентифікації, перевірка налаштувань системи та прав доступу користувачів та інше, але у випадках, коли ми кажемо про безпеку системи, краще скористатися системою безпеки та управління ризиками, що мають комплексний підхід та вже перевірені, та доповнити їх за потреби. Управління ризиками поділяється на два етапи: етап оцінки ризиків та етап зменшення ризиків. Оцінка ризиків включає визначення загроз, які можуть знищити інформаційні активи організації, та оцінку ймовірної шкоди, яку ці загрози можуть завдати системі, тоді як зниження ризиків – це етап роботи з виявленим ризиком та його усунення [37]. Зі швидким розвитком хмарних сервісів з'явилося багато моделей безпеки, і, за даними El Fray [38], ще на момент 2012 року існувало більше 200 моделей безпеки. Серед великої кількості методів є декілька, що можуть бути використані для оцінки загроз, що впливають на хмарні системи та сервіси, такі як ISO 27005, NIST SP 800-30, CRAMM, OCTAVE, CORAS та COBIT.

3.1 Моделі безпеки за стандартом ISO 27005

Стандарт ISO27005 зобов'язує організації створити команду безпеки, яка буде відповідати за розробку плану безпеки для організації. Остання редакція стандарту відбулась у 2022 році, через що було додано та змінено декілька

аспектів, таких як чітке визначення "необхідних процесів та їх взаємодію", новий розділ, що присвячено плануванню змін у СУІБ, та інші [39]. Стандарт містить систематичні кроки для управління ризиками, наведені нижче [40]:

Крок 1: Організація виконує діяльність з ідентифікації ризиків.

Крок 2: Організація виконує оцінку ризиків, які стосуються її бізнесу.

Крок 3: Команда повинна розуміти ймовірні наслідки та вплив ідентифікованого ризику.

Крок 4: Організація повинна визначити пріоритетність підходів до управління ризиками.

Крок 5: Команда повинна визначити пріоритетність дій, спрямованих на зниження ризику.

Крок 6: Організація повинна залучати зацікавлені сторони до прийняття рішень щодо управління ризиками.

Крок 7: Моніторинг обробки ризиків встановлюється на додаток до регулярного моніторингу процедури управління ризиками.

Крок 8: Команда повинна документувати всю інформацію для покращення процесу управління ризиками.

Крок 9: Організація повинна провести тренінг для персоналу організації щодо ризиків та всіх заходів, які вживаються для їх усунення.

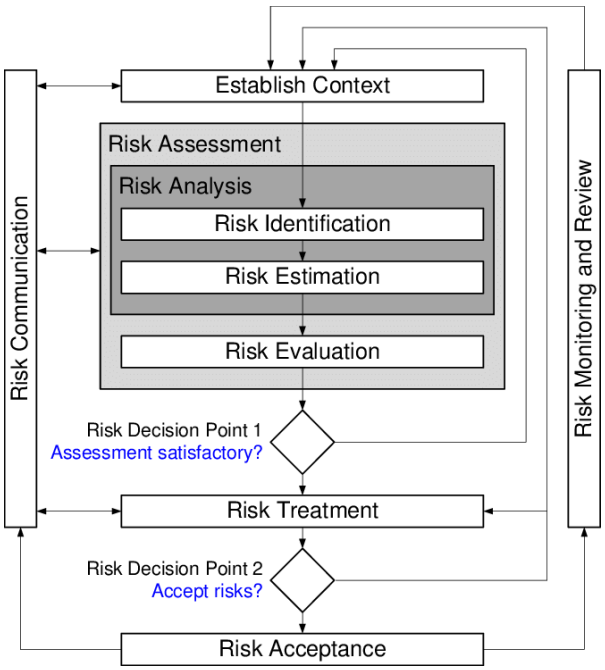

Рисунок 3.1 – Процес управління ризиками за стандартом ISO27005

Підхід, описаний у стандарті ISO27005, полягає у визначенні активів, загроз, які націлені на організацію, вразливості або слабкості, засобів контролю, ймовірності і, нарешті, наслідків [41]. На рисунку 3.1 показано процес управління ризиками за стандартом ISO27005.

3.2 Модель безпеки за стандартом NIST SP 800-30

Другим за популярністю методом управління ризиками є NIST SP 800-30. NIST може оцінити та покращити спроможність установи зупиняти, виявляти та реагувати на кібератаки, а метою Спеціальної публікації 800-30 є надання рекомендацій щодо проведення оцінювання ризиків для федеральних інформаційних систем та організацій, які доповнюють рекомендації, викладені у Спеціальній публікації 800-39. Оцінювання ризиків, що здійснюється на всіх трьох рівнях ієрархії управління ризиками, є частиною загального процесу управління ризиками, забезпечуючи вищих керівників/виконавців інформацією, необхідною для визначення відповідних заходів у відповідь на виявлені ризики. Процес управління ризиками NIST SP 800-30 включає наступні етапи [42]:

Етап 1: Організація виконує фреймінг ризиків, який полягає в побудові стратегії управління, що ілюструє, як організації хочуть оцінити ризик, щоб сформувати стратегію управління ними, яка включає в себе те, як організація буде оцінювати, реагувати і контролювати ризик.

Етап 2: На другому етапі організація проводить оцінку ризику в контексті організаційної системи ризиків, щоб визначити загрози, вразливості, шкоду, яка може статися, і ймовірність того, що така шкода станеться.

Етап 3: На третьому етапі, треба визначити, як організація реагуватиме на ризик після того, як його буде визначено під час етапу оцінки, шляхом створення кроків дій для реагування на ризик, оцінки дій, визначення належних дій і, нарешті, реалізації відповіді на основі пріоритетних дій.

Етап 4: На цьому етапі організації треба уявити, як вона буде здійснювати моніторинг ризиків, щоб відстежувати їх, а саме, щоб побачити ефективність впровадження заходів, визначити вплив змін на організацію та перевірити, що всі бажані дії впроваджуються належним чином.

Рисунок 3.2 ілюструє процес управління ризиками, що використовується в стандарті NIST SP 800-30:

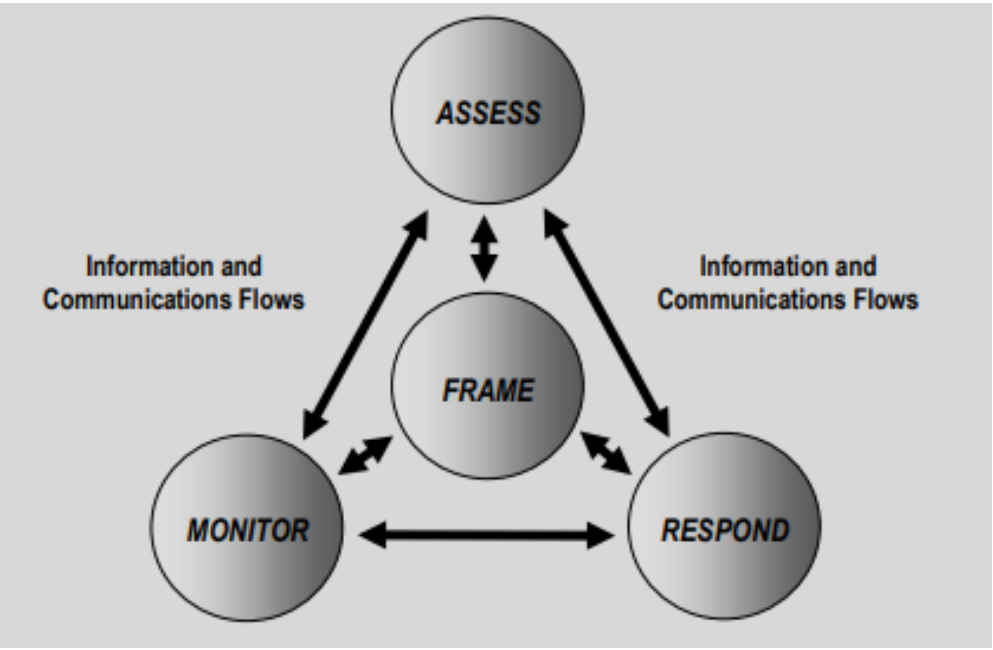

Рисунок 3.2 NIST SP 800-30

3.3 Модель безпеки Octave Allegro

Модель OCTAVE розроблена Міністерством оборони США (DOD), щоб посилити взаємозв'язок цілей і завдань організації з планами інформаційної безпеки. OCTAVE Allegro, наступна і вдосконалена редакція OCTAVE – це методологія для впорядкування та оптимізації процесу оцінки ризиків інформаційної безпеки таким чином, щоб організація могла отримати достатні результати з невеликими інвестиціями в час, людей та інші обмежені ресурси. Вона спонукає організацію розглядати людей, технології та засоби в контексті їх взаємозв'язку з інформацією та бізнес-процесами і послугами, які вони підтримують, тобто ця модель фокусується на інформаційних активах організації. Стандарт OCTAVE в основному перевіряє загрози, націлені на інформаційні активи організації, а також вразливості, які послаблюють системи і збільшують ймовірність загроз [43]. Метод OCTAVE реалізується в чотири етапи [44, 45], що проілюстровано на рисунку 3.3:

Етап 1: Організація створює критерій вимірювання ризиків для кількісної оцінки рівня їхнього впливу шляхом створення системи ранжування, яка буде використовуватися в процесі управління ризиками.

Етап 2: Організація повинна зробити два кроки. Крок 2 полягає в розробці профілю інформаційних активів, а потім, на третьому кроці, організація повинна оцінити інфраструктуру інформаційних систем, щоб визначити пріоритетність критично важливих інфраструктур та контейнерів-активів, як внутрішніх, так і зовнішніх, а також ресурсів, таких як програмне забезпечення, апаратне забезпечення, мережа та люди.

Етап 3: на цьому етапі організація реалізує два кроки, крок 4 і 5. Крок 4: організація використовує методи мозкового штурму для визначення проблемних сфер, пов'язаних з ризиками. Потім, на кроці 5, вона визначає можливий ризики, ймовірність загроз та їхній вплив, щоб підготуватися до сценаріїв загроз.

Етап 4: На цьому етапі теж необхідно виконати три кроки. Організація ідентифікує ризики на кроці 6, проводить аналіз ризиків на кроці 7 та вимірює їхній вплив для створення плану пом'якшення наслідків на кроці 8.

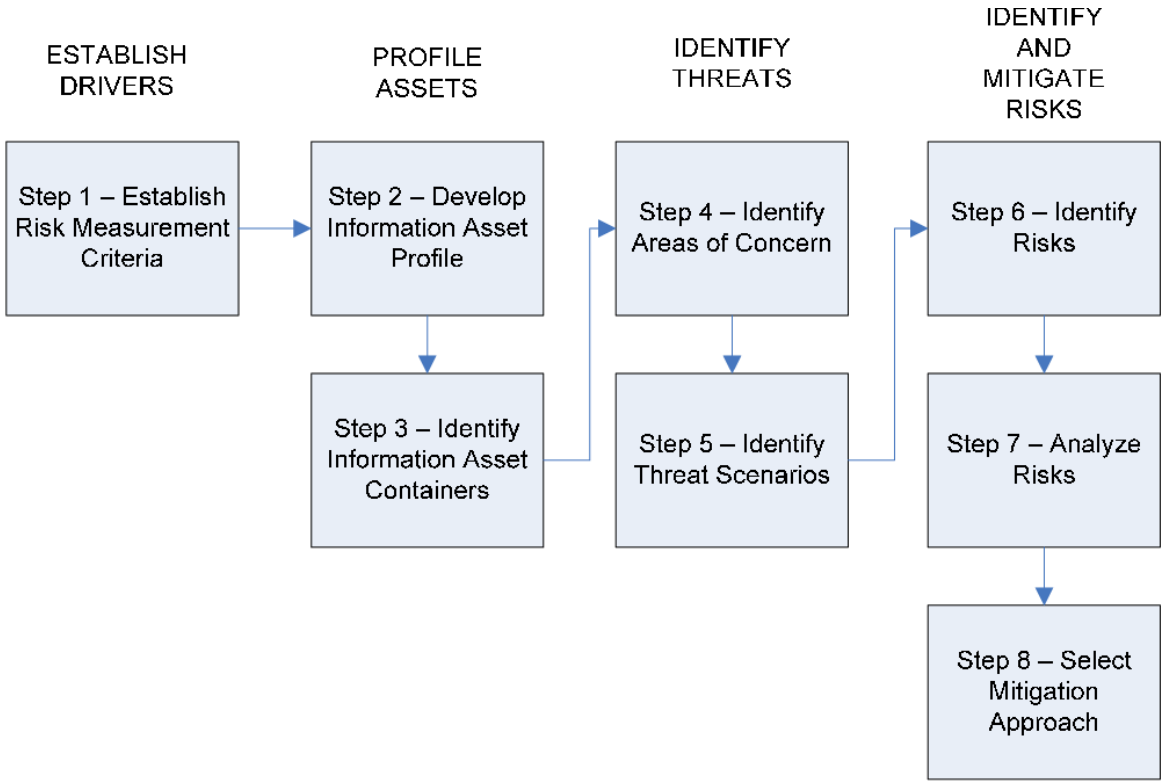

Рисунок 3.3 – OCTAVE Allegro

3.4 Підхід CRAMM

CRAMM (CCTA Risk Analysis and Management Methodology) – це підхід, розроблений британською урядовою організацією ССТА (Центральне агентство зв'язку та телекомунікацій). З такою назвою існують як метод, так і інструмент, при тому використання інструменту значно спрощує коректну роботу метода. Перші версії CRAMM (методу та інструменту) базувалися на передовому досвіді британських урядових організацій. В даний час CRAMM є основним методом аналізу ризиків, якому віддає перевагу уряд Великобританії, але CRAMM також використовується в багатьох країнах за її межами. CRAMM особливо підходить для великих організацій, таких як державні органи та промисловість [46]. У

цьому методі управління ризиками поділяється на три етапи, що проілюстровано на рисунку 3.4 [47].

Етап 1: Організація проводить ідентифікацію та оцінку активів.

Етап 2: Команда оцінює загрози, визначаючи їхній тип і рівень, що можуть вплинути на системи, а також вразливі місця. Потім, оцінивши загрози та вразливості, команда визначить міру ризику.

Етап 3: Команда розробляє та обирає стратегію пом'якшення наслідків та рекомендації.

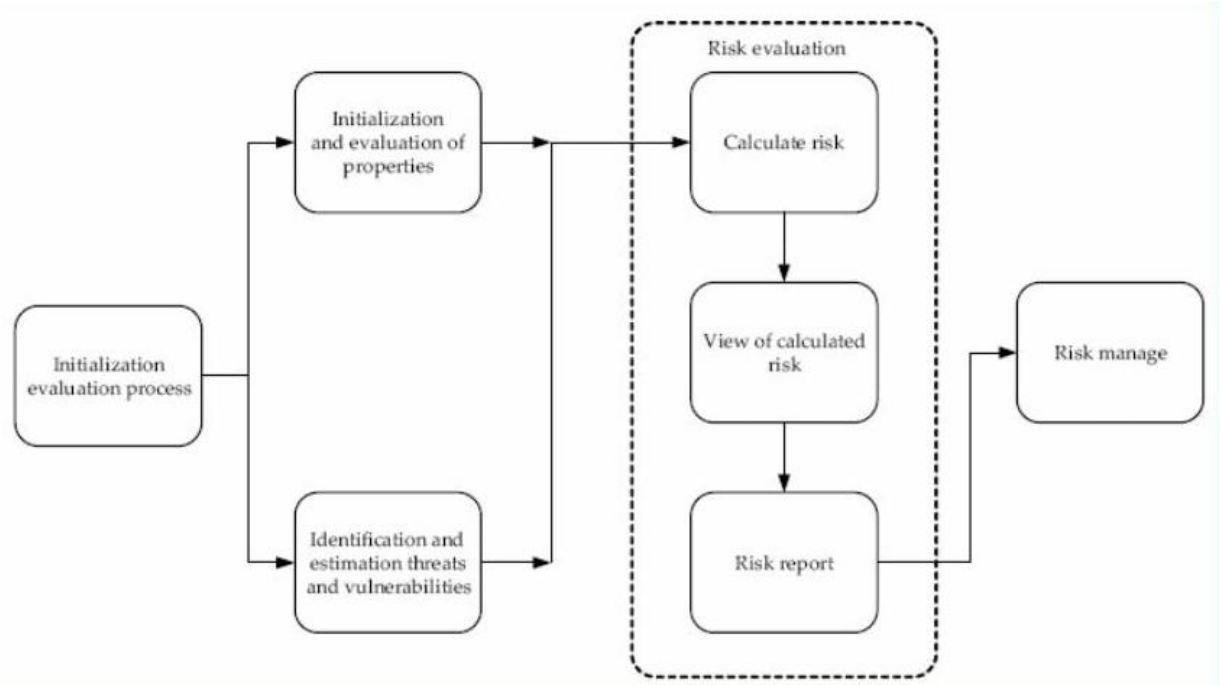

Рисунок 3.4 – CRAMM

3.5 Метод CORAS

Метод CORAS є комп'ютеризованим інструментом, що було розроблено і фінансувалось Європейською Комісією в період з 2001 по 2003 рік та призначеним для підтримки документування, збереження та звітування про результати аналізу за допомогою моделювання ризиків. Методологія CORAS створила практичну рамкову модель оцінки ризиків безпеки на основі моделей. CORAS підходить до управління ризиками у 8 етапів для аналізу безпеки [49]:

Етап 1: Першочерговою задачею є визначення основної мети та обсягу аналізу, який необхідно виконати.

Етап 2: На наступному етапі підхід вимагає зустрітися з клієнтами, для яких виконується аналіз, щоб мати уявлення про їхні потреби та вимоги. уявлення про їхні потреби та вимоги, які вони хочуть проаналізувати, щоб досягти спільного розуміння необхідного аналізу. необхідного аналізу.

Етап 3: Забезпечення взаєморозуміння щодо мети аналізу, яка включає в себе фокус, сферу застосування та активів організації.

Етап 4: Процес передбачає документальне оформлення аналізу, що містить основну мету, фокус і завдання правильно визначені та коректні.

Етап 5 включає визначення ризиків за допомогою мозкового штурму, обговорення та семінарів з відповідними особами.

Етап 6 – це визначення рівня ризику на основі попереднього кроку для оцінки впливу ризику.

Етап 7: Організація визначає, з якими ризиками можна погодитися, а з якими потрібно боротися і які потребують подальшого опрацювання.

Етап 8: Організація визначає та оцінює методи лікування.

Варто зазначити, що цей підхід побудовано на основі UML (Unified Modelling Language – уніфікована мова моделювання), яка є мовою, що застосовує діаграми для пояснення взаємозв'язків та кореляції між користувачами та навколишнім середовищем [43]. А оскільки він містить моделювання загроз для програмного забезпечення та розподілених систем, це робить CORAS адаптованим до хмарних систем [48].

Рисунок 3.5 нижче ілюструє підхід методології CORAS.

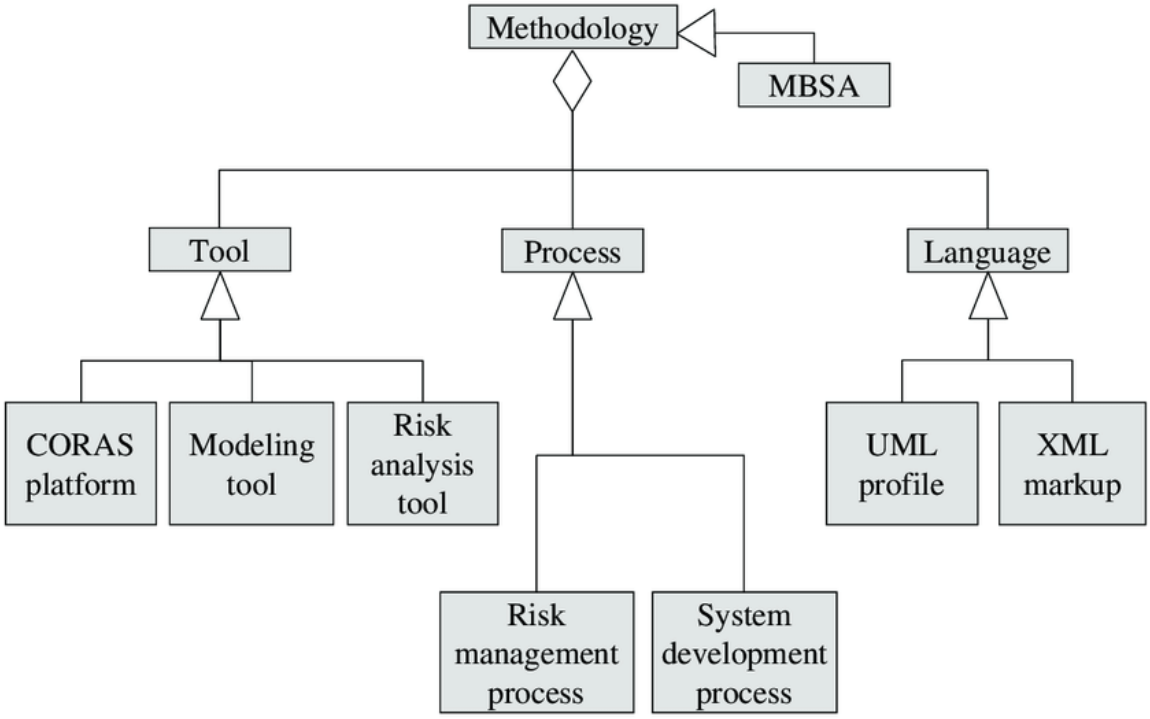

Рисунок 3.5 – CORAS

3.6 Модель COBIT-2019

Запущена в 2012 році, модель цілей контролю інформаційних та суміжних технологій (COBIT 5) – це модель, розроблена Асоціацією аудиту та контролю інформаційних систем (ISACA), яка допомагає в управлінні ризиками та оцінці ризиків для інформаційних активів організації, розміщених у хмарі для інформаційних активів організації, розміщених у хмарі, та впливу цих ризиків на організацію [50]. Її було оновлено у 2019 році, та це є та версія, що використовується зараз. Основні зміни включають нову публікацію в рамках основної структури, кілька нових цілей, оновлення практик безпеки та оновлені посилання на інші стандарти, керівництва та нормативні акти.

Невід'ємною частиною суті системи є 6 системних принципів EGIT (рисунок 3.6). Вони є основою успіху системи, і кожен, хто керує розвитком EGIT в компанії, повинен часто посилатися на них. Хоча "наскрізне управління" здається очевидним, на цьому шляху може статися багато помилок, і жодна з 6 концепцій не повинна бути пропущена, щоб завершити шлях інтеграції

фреймворку для отримання переваг від ради директорів та її керівників до членів IT-команди та інших зацікавлених сторін [51].

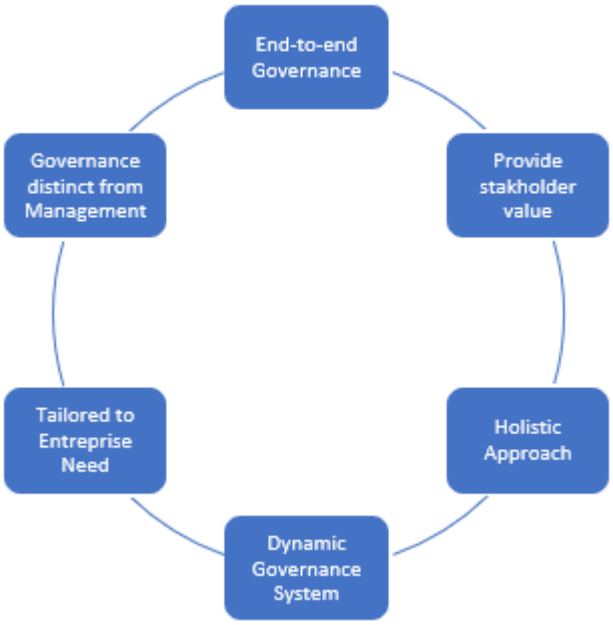

Рисунок 3.6 – 6 принципів системи управління

Для того, щоб розробити індивідуальну структуру для будь-якої компанії, яка бажає впровадити ефективну систему безпеки, COBIT розробив наскрізний процес, в основі якого лежить Базова модель COBIT, центральним елементом якої є Цілі управління та менеджменту.

Вхідні дані для цієї базової моделі мають бути отримані не лише з інших нормативно-правових актів, а й від зацікавлених сторін компанії. Ці вимоги призводять до низки цілей, які мають бути досягнуті на основі факторів проектування та пріоритетних напрямків. Потім, результати всього цього стратегічного дизайну допомагають перейти до Спеціальної системи управління підприємством, яку необхідно впроваджувати, контролювати та управляти нею для досягнення бажаних цілей та результатів діяльності EGIT.

Щоб гарантувати найкраще впровадження, для цієї нової версії було опубліковано певну кількість основних публікацій COBIT: від заснування до управління, а також від розробки до впровадження, включаючи покрокове розуміння та навчальні документи.

Основну модель показано на рис. 3.7. Вона містить 40 цілей врядування та управління, що розділено на 5 сфер, потрібних для спрямовування, структуризації та стимуляції роботи:

A. Область цілей врядування:

1) Оцінювання, управління та моніторинг (ОУМ) – 5 цілей

B. Домени цілей управління:

1) Узгоджувати, планувати та організовувати (APO) – 14 цілей
2) Створювати, купувати та впроваджувати (BAI) – 11 цілей
3) Надавати, обслуговувати та підтримувати (DSS) –6 цілей
4) Моніторинг, оцінка та аналіз (MEA) – 4 цілі

Ключовим елементом, про який слід пам'ятати, є те, що COBIT не є директивним документом і не вказує, ЯК досягти цих цілей, але забезпечує структуру для виведення врядування на новий рівень ефективності.

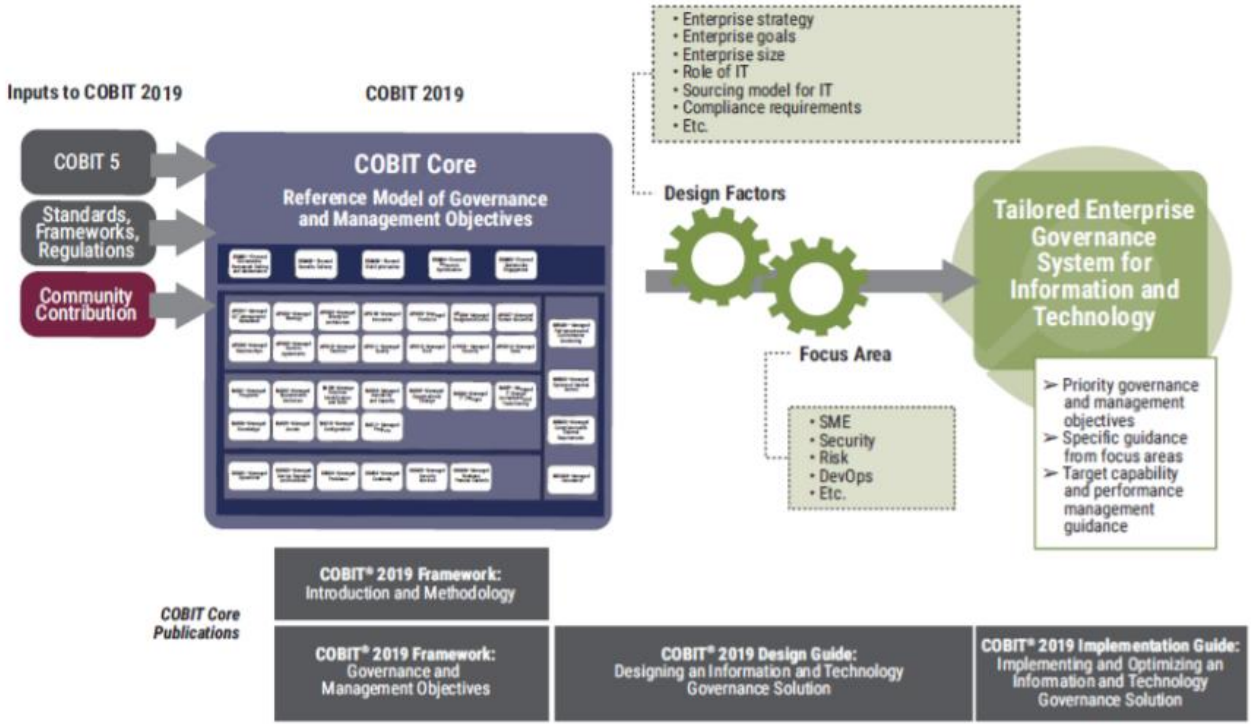

Рисунок 3.7 – Основна модель COBIT 2019

Вище було перераховано найбільш поширені методи управління ризиками, та їх основні характеристиками. У висновок можна сказати, що OCTAVE Allegro можна визначити як найкращу модель для хмарного хостингу, а також доволі повними COBIT 2019 і CORAS з певним налаштуванням. Попередні моделі підтримують тріаду ЦРУ і зосереджені на зберіганні, обробці та передачі інформації. Стандарти ISO27005, NIST SP 800-30 та CRAMM описують управління та оцінку ризиків абстрактно і можуть не надавати чітких вказівок щодо оцінки та аналізу хмарних ризиків, на відміну від моделей безпеки OCTAVE, CORAS і COBIT2019, що мають чіткий процес управління ризиками, пов'язаними як із зовнішніми, так і з внутрішніми системами та програмними ресурсами. Крім того, вони включають специфічну для хмар інфраструктуру, таку як контейнери та інші ресурси, при оцінці ризиків, що теж є важливим аспектом забезпечення безпеки в хмарі. Також COBIT 2019 додатково охоплює частину управління при роботі з хмарними системами. З іншого боку, ISO27005, NIST SP 800-30 та CRAMM – це абстрактні підходи високого рівня, які забезпечують загальний процес управління ризиками, не зосереджені на хмарній інфраструктурі, але можуть бути використовуваними там з додатковими дослідженнями для інтеграції та адаптації.

4 МОДЕЛІ ЗАГРОЗ, ПОРУШНИКА ТА БЕЗПЕКИ ХМАРНИХ СЕРВІСІВ

UcedaVelez та Morana [52] визначають моделювання загроз додатків як "стратегічний процес, спрямований на розгляд можливих сценаріїв атак та вразливостей у запропонованому або існуючому середовищі додатків з метою чіткого визначення рівнів ризику та впливу". Gupta та ін. [53] розглядають моделювання загроз як спосіб захисту системи, аналізуючи її з точки зору зловмисника, щоб визначити різні методи, які можуть призвести до порушення безпеки таких важливих властивостей, як доступність, цілісність і конфіденційність. У контексті гнучкої розробки програмного забезпечення Бернсмед та ін. [54] описують моделювання загроз як ключову діяльність для створення програмного забезпечення, яке підтримує функціонування відповідно до плану, в тому числі під час кібератак. Згідно з Xiong та Lagerstrong [55], "Моделювання загроз – це процес, який може бути використаний для аналізу потенційних атак або загроз, а також може бути підтриманий бібліотеками загроз або таксономіями атак". Як можна побачити, існує дуже багато визначень моделей загроз, що об’єднані спільним терміном, але освічують його з різних сторін. Загалом, мабуть, можна сказати, що модель як загроз, так і безпеки та порушника, слід створювати і розуміти шляхом формулювання детального уявлення про середовище, активи, процеси та дійових осіб для моделювання необхідних заходів з пом'якшення наслідків.

4.1 Моделювання загроз

Як було зазначено вище, моделювання загроз має на увазі ретельне вивчення вразливостей системи з боку зловмисника, який може ними скористатись, а результатом цього процесу є абстрактний структурований опис загроз. Модель дозволяє архітекторам програмного забезпечення виявляти та пом'якшувати потенційні проблеми безпеки на ранніх стадіях, коли їх відносно

легко та економічно ефективно вирішити. Як результат, це значно знижує загальну вартість розробки та підвищує її безпеку. Загальна схема моделювання загроз наведена на рис. 4.1, і саме за таким алгоритмом зазвичай працюють усі схеми моделювання загроз. Існує також загальна модель загроз для хмарних обчислень, яку наведено на рис. 4.2 [65]. Однак, вона не є ідеальною, хоча й дає досить чітке уявлення про можливі ризики та загрози та дає можливість потенційно їх оцінити. Слід зазначити, що в ідеалі модель загроз повинна брати до уваги модель розгортання та обслуговування, але зазвичай організації обмежуються більш загальним аналізом.

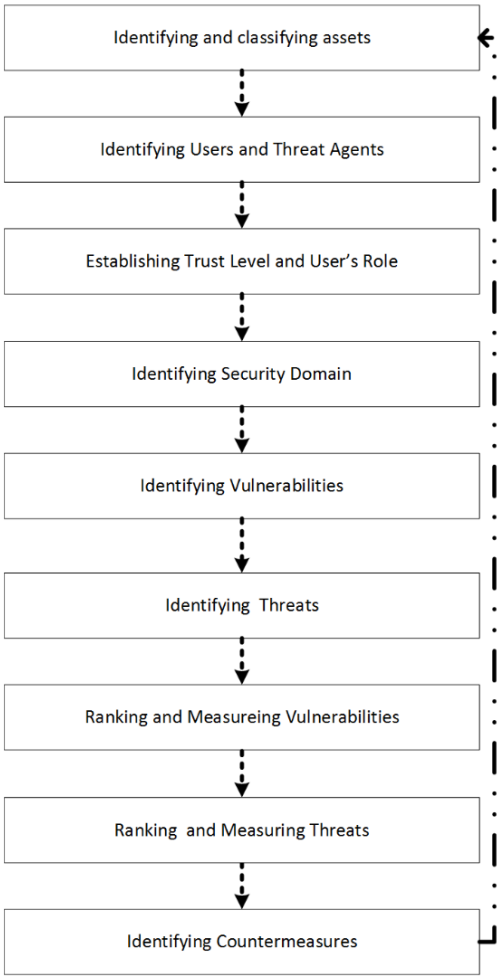

Рисунок 4.1 – Загальна схема моделювання загроз

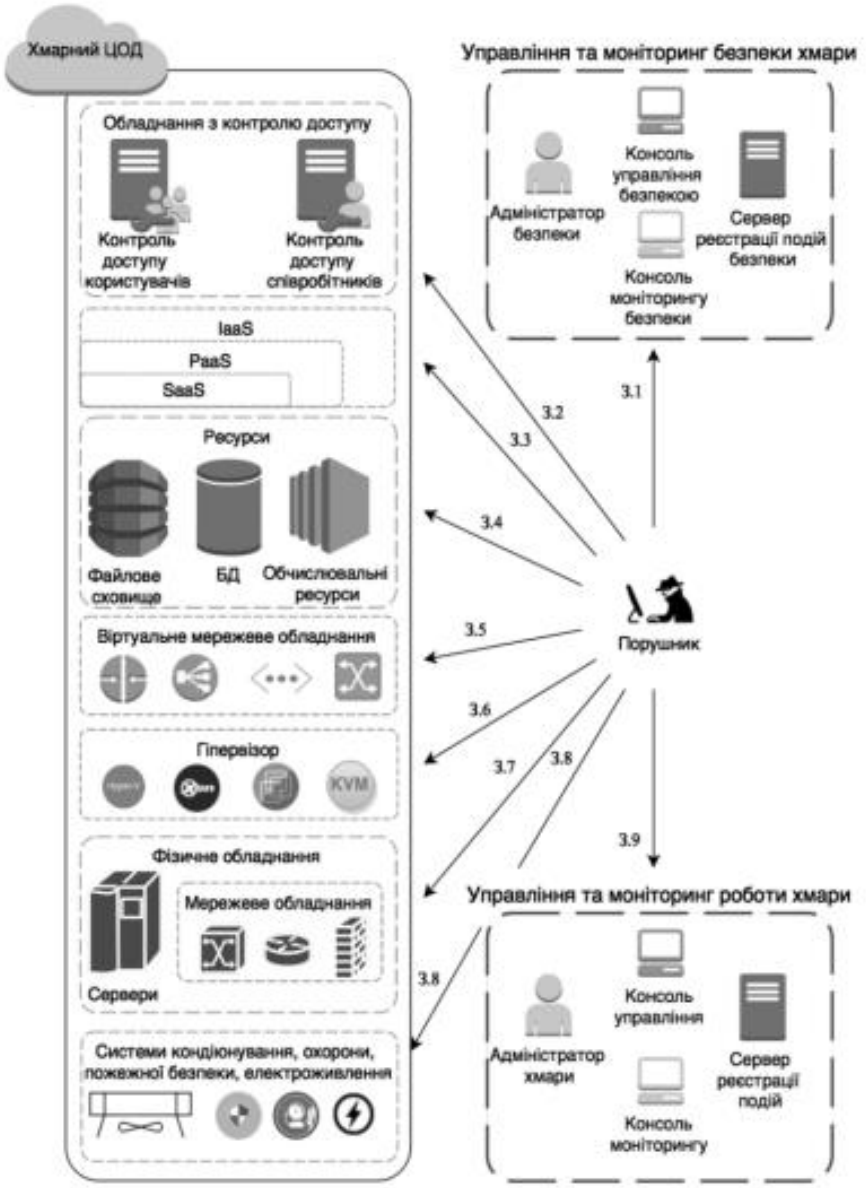

Рисунок 4.2 – Модель загроз хмарних обчислень

У наведеній на рис. 4.2 моделі розібрано об’єкти, для яких реалізується загроза, мета порушника та можлива мета здійснення захисту. Найбільшу небезпеку складають загрози управління хмарою, безпекою хмари та загрози гіпервізору, а найбільш вірогідними, згідно з аналізом – загрози, що спрямовані на ті компоненти хмарної архітектури, що знаходяться в віртуалізованому середовищі.

Серед найбільш популярних та використовуваних слід зазначити також модель STRIDE [63] – така модель, що може бути використана для візуалізації мережевих та інфраструктурних загроз, отриманих з огляду архітектури та потоків даних. STRIDE отримала свою назву від абревіатури груп загроз, які вона використовує для своєї класифікації (підробка, втручання, заперечення, розкриття інформації, відмова в обслуговуванні та підвищення привілеїв). Вона, мабуть, є однією з найбільш поширених, не дивлячись на деякі її недоліки.

Spoofing – підробка – це порушення автентичності.

Tampering – порушення цілісності.

Repudiation – Ствердження, що ви не виконували якусь дію.

Information Disclosure – Розкриття інформації є порушенням конфіденційності.

Denial of Service – Відмова в обслуговуванні (DoS) є порушенням доступності.

Elevation of Privilege – Підвищення привілеїв є порушенням авторизації.

Наведений метод ґрунтується на діаграмі та впроваджених засобах контролю безпеки, щоб перерахувати різні методи, які можуть бути використані зловмисником, незалежно або в поєднанні один з одним, щоб скомпрометувати систему. Microsoft розробила його ще в 1999 році, і не дивлячись на те, що більше окремо він не підтримується та має деяких противників (що стверджують, що цей метод та подібні йому мають багато вразливостей), він все ще є використовуваним та заслуговує на згадування.

Система Лукаса Руфа [64] – ще одна спроба класифікувати загрози – надає модель, яка намагалася класифікувати загрози на основі трьох понять: агент (загроза для системи – людина, технологія тощо), локалізація (внутрішня чи зовнішня загрози) та мотивація.

Схожу на попередньою модель пропонує CSA – вони посилаються на Cloud Top Threats Deep Dives Egregious Eleven [66] та пропонують класифікацію за

наступними категоріями: діюча особа, атака та вразливість. Загальна схема зображена на рис. 4.3.

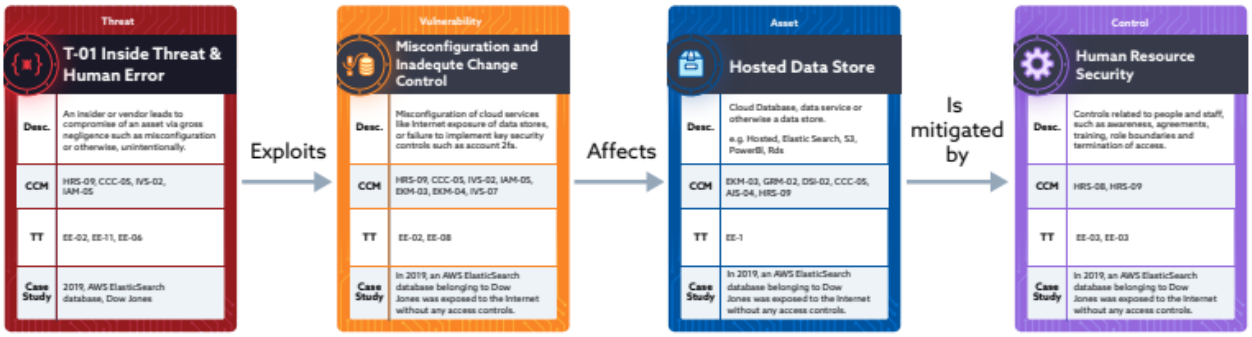

Рисунок 4.3 – Модель загроз, пропонована CSA

Серед цікавих для вивчення, але, на жаль, рідко використовуваних слід зазначити модель, що пропонували Манзур та ін. [62]. Вона основана на мережі Петрі для ретельного профілювання операційної поведінки сервісів, за допомогою чого їхній метод може моделювати загрози як на одному рівні, так і на різних, а також виявляти вразливості, щоб зменшити поверхню атаки хмари. Однак, це дуже дорогий доменний підхід, що значно зменшує його застосованість.

Сааткамп та ін. [57] запропонували підхід до впровадження політики безпеки, орієнтований на мінімізацію загроз, і надали методику на основі TOSCA, щоб допомогти архітекторам протягом усього процесу моделювання. Такий підхід допомагає користувачеві вибрати можливі абстрактні функції пом'якшення наслідків, зіставлені з конкретною реалізацією, і автоматично вставляє відповідні мережеві функції безпеки в модель розгортання. Їхній метод передбачає шість кроків із залученням архітектора та експерта з безпеки, перш ніж модель розгортання стане готовою для надання послуг. Цій моделі, на жаль, бракує достатньої формалізації і автоматизації ідентифікації загроз.

Бражук [56], щоб вирішити цю проблему, запропонував більш формальний фреймворк, заснований на онтології, який отримав назву OdTM. OdTM розроблено для моделювання загроз для конкретної предметної області, представленої діаграмою потоків даних, та він має широкі можливості

застосування – від аналізу дизайну системи до генерації шаблонів безпеки, використовуючи контекстно-орієнтовані шаблони безпеки.

Для вирішення тієї ж проблеми Cauli та ін. [58] запропонували підхід, який використовує логіку опису для моделювання загроз, щоб підвищити безпеку хмарних установок. Цей метод використовує декларативну мову CloudFormation, розроблену Amazon Web Services, на чому засновано інструмент, що перетворює файли шаблонів у логіку. Автори застосували більш ретельні семантичні міркування, щоб допомогти в оцінці безпеки, доповнивши моделі специфічними для потоку даних знаннями.

Існує ще безліч різних моделей загроз, що базуються на різних принципах та застосовують різні методи, але мають одну мету – запобігти усім можливим загрозам та зменшити потенційні втрати даних. Вище наведено як загально використовувану модель загроз та алгоритм створення будь-якої моделі, так і інші пропоновані моделі, що мають інший підхід для моделювання загроз.

4.2 Модель порушника

Модель порушника визначається як абстрактний опис дій порушника, який відображає та дає уяву про його практичні та теоретичні можливості, його мету, знання та повноваження в системі та інше.

Складання моделі порушника для хмарних сервісів є складнішим, ніж для фізичної системи, оскільки така модель потребує враховувати як моделі розгортання і обслуговування хмари, так і власника інформації та хмари, бути симетричною реальному порушнику та ін.

Зазвичай профіль порушника визначає такі категорії [65]:

- Залученість

Це допомагає визначити, ким є порушник – зовнішній або внутрішній користувач хмари

- Характер дій зловмисника

Він буває випадковим, пасивним чи активним. Наприклад, пасивним порушником вважається людина, що свідомо зламала систему, але не вживає рішучих дій, що можуть призвести до великих збитків, активний займається саме цим, а випадковий не мав мети зламати систему, але якось це зробив.

- Рівень доступу до інформації

Мається на увазі легально наданий рівень доступу, який має авторизований користувач.

- Рівень ознайомлення з системою – користувач, спеціаліст, адміністратор системи/безпеки тощо

Аналіз та практика показують, що найбільш небезпечним є адміністратор безпеки, тому людей, що займають ці посади, слід перевіряти та відноситись до виконання ними їхніх обов'язків дуже ретельно.

- Використовувані методи та засоби – пасивні та активні; агентурні та штатні
- Мета дій порушника

Мабуть, найбільш невизначений пункт, бо, як відомо, мета дій може бути будь-якою. Однак, зазвичай виділяють наступні: отримання несанкціонованого доступу до ресурсів, проникнення з метою впливу на фізичне обладнання, встановлення засобів технічної/програмної розвідки або нав'язування, вивід з ладу фізичних чи хмарних ресурсів та інше.

Використання моделі порушника дозволяє формалізувати процес побудування загроз хмари та аналіз можливий дій порушника, та, як висновок, покращити систему безпеки та передбачити можливі результати атак та втрати.

4.3 Модель безпеки

Як було зазначено ще в першому розділі, різні моделі розгортання та обслуговування відрізняються одна від одної не лише своїми можливостями, а ще й рівнем безпеки, що вони мають, а ще й рівнем відповідальності, яку несуть постачальник чи користувач хмарних послуг. У будь-якій системі, що

використовує хмарні сервіси, неможливо перекласти обов’язки по забезпеченню безпеки лише на одну сторону, оскільки вразливості існують з двох боків і саме тому для найбільш повного та комплексного підходу для уникнення ризиків застосовується так звана модуль спільної відповідальності. Зазвичай відповідальність користувачів зростає в міру їх переходу від SaaS до PaaS і IaaS. У даній моделі зазвичай виділяють окремо основні обов’язки користувача та постачальника, що не залежать від обраної моделі, але деякі є мінливими та залежать від моделі [67].

Загалом, на користувача покладається відповідальність за налаштування та конфігурації, що знаходяться під його контролем. Типові обов'язки замовника включають контроль наступних аспектів:

- Захист додатків, даних та облікових даних

Користувачі повинні контролювати доступ до даних, що вони завантажують в мережу, наприклад, за допомогою шифрування даних або створення різних рівнів доступу та авторизацій для них. До цього пункту відноситься контроль середовища IAM: наприклад, елементів багатофакторної ідентифікації, ключів шифрування, механізмів входу тощо. Те саме стосується й додатків, що розміщено у хмарній віртуальній машині, а також – будь-яких підключених систем, як-то локальні бази даних чи інші навантаження.

- Конфігурації

Існує низка проблем, пов’язаних з неправильною конфігурацією системи. Її налаштування – зазвичай складний та трудомісткий процес, що виконується за допомогою інструментів та опцій провайдера, але він є необхідним для безпечного існування системи.

- Зовнішні підключення

Зазвичай у хмару перекосять не всю систему організації, а лише її частку, тому користувачам слід пам’ятати, що за традиційну інфраструктуру, що не була перенесена, вони несуть відповідальність самі.

Хмарні провайдери, в свою чергу, несуть відповідальність за усю інфраструктуру, що вони постачають. До їх сфери відповідальності відносять контроль наступних елементів:

- Фізичний аспект

Провайдер має захищати елементи своєї фізичної інфраструктури, як-то сервера, приміщення, мережеве обладнання та інше. Зазвичай розвинена інфраструктура включає в себе відмовостійкість, резервування, резервні живлення, копіювання, та підключення до оператору зв’язку.

- Рівень віртуалізації

Деякі користувачі хмарних сервісів, мабуть, вважають їхні можливості майже необмеженими: миттєве змінення навантажень, ресурсів, використовуваних сервісів. Але для забезпечення такої картини постачальники хмарних послуг треба зробити та забезпечити високий рівень віртуалізації та автоматизації створеної ними системи. Провайдер відповідає за впровадження та підтримку цього рівня віртуалізації/абстракції, а також різноманітних API, які слугують засобом доступу користувачів до інфраструктури та взаємодії з нею.

- Безпека пропонованих послуг

Окрім забезпечення безпеки фізичного середовища, провайдер має ще й відповідати за безпеку впроваджених послуг – операційних систем, додатків, серверів тощо.

Як було зазначено вище, деякі обов’язки можуть відноситись до різних сторін в залежності від обраної моделі розгортання чи обслуговування та ще деяких деталей. До таких невизначених елементів відносять наступні:

- Власний чи сторонній розробник

Для клієнта важливо, хто створює послугу (провайдер чи сам він), бо творець несе відповідальність за безпеку. Наприклад, при використанні пропонованої розробником бази даних, за її розгортання, підтримку, управління тощо несе відповідальність постачальник послуг (але за управління та захист

розташованих там даних – все одно клієнт, як було зазначено вище). У випадку, коли клієнт сам розробляє базу даних, розгортаючи її як навантаження у хмарному екземплярі, зазначені вище обов’язки переходять на його відповідальність, а постачальнику лишається лише контроль над інфраструктурою та рівнем віртуалізації.

- Серверні чи безсерверні обчислення

Якщо користувач хмари обирає традиційну серверну віртуальну машину, він відповідає за вибір операційної системи, розгортання робочого навантаження та будь-які пов'язані з цим налаштування безпеки/конфігурації. Якщо користувач хмари обирає безсерверні (засновані на подіях) обчислення, користувач несе відповідальність за код, завантажений на сервіс, а також за будь-які параметри безпеки/конфігурації користувача, що надаються через площину управління.

- Управління мережею.

Розглянемо мережевий сервіс, такий як брандмауер. Незалежно від того, чи користувач розгортає брандмауер самостійно, чи користується послугою брандмауера від провайдера, користувач несе відповідальність за встановлення правил брандмауера та забезпечення належної конфігурації брандмауера для захисту пов'язаних з ним додатків користувача або інших мережевих елементів.

- Операційні системи.

Незалежно від того, чи користувач використовує власну ОС, чи розгортає ОС, надану провайдером, користувач зазвичай вирішує, яку ОС використовувати, і це рішення тягне за собою низку інших проблем безпеки. Користувач несе відповідальність за те, щоб ОС була належним чином сконфігурована з відповідними налаштуваннями безпеки і належним чином виправлена відповідно до вимог безпеки.

Хмарні технології набувають є достатньо молодою технологією, тож використана ними модель спільної відповідальності, хоча і є широко використовуваною, може здатись заплутаною та має свої переваги та недоліки.

Переваги:

- Простота

Завдяки спільній відповідальності стає очевидним той факт, що для кожної зі сторін кількість задач, про яку вони повинні піклуватись, зменшується, що дозволяє більш зосередитись саме на виконанні обов’язків.

- Обізнаність та досвід

Хмарні провайдери приділяють багато уваги забезпеченню безпеки, що може бути плюсом для організацій, які з будь-яких причин не мають власних фахівців з безпеки або їх замало.

Однак, обираючи хмарні сервіси, користувачі мають ретельно проаналізувати недоліки та ризики, що постають через недоліки такої системи:

- Необхідність довіри

Модель спільної відповідальності розподіляє обов’язки з захисту даних, тому користувачам слід бути впевненими, що постачальник виконує свої обов’язки так, як це було зазначено, і що зазначений у договорі рівень безпеки є достатнім для компанії, яка, наприклад, розміщує конфіденційні дані в хмарі.

- Необхідність обізнаності

Для забезпечення надійності з боку користувачів требі, щоб вони добре знались та розуміли використовувані системи, їхні інструменти та будову та розуміли відмінності такої моделі від класичної. Цей пункт здається не дуже важким та зрозумілим, але саме через недотримання нескладних вимог трапляється багато витоків чутливої інформації. Також системи хмарних сервісів постійно оновлюються, та користувачі повинні відслідковувати ці зміни для забезпечення захисту своїх даних, конфігурацій та налаштувань.

- Відповідальність через виток інформації

Перенесення робочих навантажень і даних у хмару та використання моделі спільної відповідальності, на жаль, не виключає вірогідності хакерських атак. Тому при обранні слід враховувати як цей факт, так і те, що типові угоди про

рівень обслуговування (SLA) зазвичай звільняють провайдера від відповідальності за будь-які упущення чи помилки у сфері безпеки.

ВИСНОВКИ

Хмарні сервіси є невід’ємною частиною нашого життя у сьогоднішні часи, та вони ставатимуть ще популярнішими у найближчі часи. Саме через постійний розвиток та збільшення кількості користувачів та пропонованих послуг вони є дуже цікавим об’єктом для вивчення, але у популярності є, на жаль, інша сторона. Саме через неї та те, що користувачі довіряють хмарам чутливі дані, хакери та зловмисники шукають та користуються усіма можливими вразливостями та недоліками безпеки, саме тому дуже важливо вивчати тему запобігання цим ризикам, що і було темою моєї роботи.

У ході виконання атестаційної роботи бакалавра було проведено дослідження ризиків хмарних сервісів та виконано усі поставлені завдання. В результаті дослідження ми дізнались, що:

Хмарні сервіси мають різні моделі обслуговування та моделі розгортання, що відрізняються як спектром та глибиною наданих послуг, так і кількістю користувачів одних й тих самих ресурсів, що значно впливає на безпеку хмарного середовища. Різні моделі обслуговування, як-то IaaS, PaaS, SaaS дозволяють перекласти різну кількість обов’язків з обслуговування, збірки та оновлень локальної системи для організації та тим самим значно спростити їхнє життя. Моделі розгортання дозволяють корегувати кількість організацій-користувачів хмари та їхню доступність у загальній мережі.

Як було вже зазначено вище, основною проблемою хмарних сервісів є саме загрози безпеки, тому необхідно класифікувати ризики, які можуть перешкоджати ефективності бізнес-процесів, розгорнутих у хмарі, для кращого їм запобігання. Існує багато різних моделей класифікації загроз, та кожна має свої переваги та недоліки, але у роботі було розглянуто ту систему, що надає найбільш повну класифікацію за результатами досліджень. Вона має назву таксономії ризиків безпеки хмарних обчислень та поділяє ризики на шість

категорій – це безпека даних, логічний доступ, мережева безпека, фізична безпека, відповідність вимогам і віртуалізація.

Звісно, класифікація ризиків дозволяє використовувати методи захисту для кожної з категорій ризику, але краще скористатись комплексною системою, яка точно враховує все. Саме тому у третьому розділі проаналізовано деякі популярні системи захисту та зроблено висновки щодо їхньої продуманості та застосованості, бо різні моделі надають різні вказівки: ISO27005, NIST SP 800-30 та CRAMM описують управління та оцінку ризиків абстрактно і можуть не надавати чітких вказівок щодо оцінки та аналізу хмарних ризиків, на відміну від моделей безпеки OCTAVE, CORAS і COBIT2019, що мають чіткий процес управління ризиками, пов'язаними як із зовнішніми, так і з внутрішніми системами та програмними ресурсами. Найкращею системою, у висновок, слід зазначити OCTAVE Allegro, оскільки вона є найбільш повною та включає специфічну для хмар інфраструктуру, таку як контейнери та інші ресурси, при оцінці ризиків (так само, як і COBIT 2019 і CORAS, однак вони потребують додаткових налаштувань).

У результаті було проаналізовано також різні моделі загроз, а також моделі порушника та безпеки, та слід зазначити, що найбільш застосованою слід вважати загальну модель загроз (рис. 4.2), оскільки вона є найбільш універсальною. Модель порушника досить дозволяє досить однозначно класифікувати можливого порушника, а модель безпеки – модель спільної відповідальності – достатньо чітко розподіляє сфери обслуговування та зони відповідальності хмарних сервісів.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology, Vol.53,no.6, p. 50, 2009
2. Хмарні обчислення. *Integrity Systems*. URL: http://integritysys.com.ua/solutions/pricatecloud-solution/ (дата звернення: 30.03.2023).
3. Kita, Chigusa. J.C.R. Licklider's vision for the IPTO. Annals of the History of Computing, IEEE. (2003). 25. 62 - 77. 10.1109/MAHC.2003.1226656. (дата звернення: 30.03.2023).
4. Memorandum For Members and Affiliates of the Intergalactic Computer Network « Kurzweil. *Kurzweil*. URL: https://www.kurzweilai.net/memorandum-for-members-and-affiliates-of-the-intergalactic-computer-network (дата звернення: 20.03.2023).
5. Rosencrance L. SaaS vs. IaaS vs. PaaS: Differences, Pros, Cons and Examples. *WhatIs.com*. URL: https://www.techtarget.com/whatis/SaaS-IaaS-PaaS-Comparing-Cloud-Service-Models (дата звернення: 27.03.2023).
6. Top 3 Cloud Computing Service Models: SaaS | PaaS | IaaS. *K21Academy | Azure, AWS, Oracle & Google Cloud Online Training*. URL: https://k21academy.com/amazon-web-services/aws-solutions-architect/cloud-service-models/ (дата звернення: 30.03.2023).
7. Top 3 Cloud Computing Service Models: SaaS | PaaS | IaaS. *K21Academy | Azure, AWS, Oracle & Google Cloud Online Training*. URL: https://k21academy.com/amazon-web-services/aws-solutions-architect/cloud-service-models/ (дата звернення: 31.03.2023).

8. Найкращі хмарні сервіси України у 2022 році: дослідження Molfar. *AIN.UA*. URL: https://ain.ua/2022/09/15/najkrashhi-hmarni-servisy-ukrayiny-u-2022-roczi-doslidzhennya-molfar/ (дата звернення: 30.03.2023).
9. Що таке хмарні сервіси та як вони допомагають бізнесу?. *GigaCloud: Хмарні технології та хмарний сервіс для бізнесу*. URL: https://gigacloud.ua/blog/navchannja/scho-take-hmarni-servisi-ta-jak-voni-dopomagajut-biznesu (дата звернення: 1.04.2023).
10. Платформа для обміну файлами й особисте хмарне сховище – *Google*. URL: https://www.google.com/intl/uk_UA/drive/ (дата звернення: 30.03.2023).
11. Тепер Office називається Microsoft 365 – *Microsoft.* URL: https://www.microsoft.com/uk-ua/microsoft-365/microsoft-office (дата звернення: 6.04.2023).
12. Serpstat – #1 Keyword Research and Competitor Analysis Tool. *Serpstat – Growth Hacking Tool for SEO, PPC and Content Marketing*. URL: https://serpstat.com/uk/about/ (дата звернення: 5.04.2023).
13. Deals - Система електронного документообігу. Системи управління електронними документами на ринку України. Українські системи документообігу1. *Deals – майбутнє документообігу*. URL: https://dealssign.com/ (дата звернення: 08.04.2023).
14. OSINT-спільнота Molfar – *Molfar*. URL: https://www.molfar.global/ (дата звернення: 1.04.2023).
15. Molfar. Report UA. Google Docs. URL: https://docs.google.com/ (дата звернення: 15.03.2023). document/d/1WMPId_iLep8v1u_QWlXjYLVjqym F9PjZ9IeqHow8VNQ/edit (дата звернення: 11.04.2023).
16. Weitz, C, Hindley, N, Ilse, R. A Balancing Act: What Cloud Computing Means for Business, and How to Capitalize on It. *Deloitte SA*.

URL: https://deloittesa.files.wordpress.com/2010/09/a-balancing-act-what-cloud-computing-means-for-business1.pdf (дата звернення: 19.04.2023).

17. Gregg, M. 10 Security Concerns for Cloud Computing. *www.globalknowledge.com*. 2010 (дата звернення: 19.04.2023).
18. Rittinghouse J. W., Ransome J. F. Cloud Computing: Implementation, Management, and Security. Taylor & Francis Group, 2017. 340 p. (дата звернення: 15.05.2023).
19. Sun Y., Zhang zhangjs J., Xiong Y., and Zhu G. (2014) "Data Security and Privacy in Cloud Computing". (дата звернення: 13.05.2023).
20. Єсіна М, Кравченко А., Кравченко С. ОГЛЯД ЗАГРОЗ БЕЗПЕЦІ ТА ЦІЛІСНОСТІ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ. Подано до журналу *Радотехніка*. 2023. (дата звернення: 25.05.2023).
21. Chou T. "Security threats on cloud computing vulnerabilities", *International Journal of Computer Science & Information Technology (IJCSIT)* Vol 5, No 3, June 2013, pp. 84-85. (дата звернення: 15.05.2023).
22. Kaur R., Pateriya P., "A Study on Security Requirements in Different Cloud Frameworks", *International Journal of Soft Computing and Engineering (IJSCE)* 2013, ISSN: 2231-2307, Volume-3, Issue-1, pp.134-135. (дата звернення: 15.05.2023).
23. Mohapatra H., "Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System," *Int. J. Emerg. Trends Eng. Res.*, 2020, vol. 8, no. 5, pp. 1503–1510. (дата звернення: 16.05.2023).
24. What is a DDoS attack? Microsoft – *Microsoft.* URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack. (дата звернення: 19.04.2023).
25. Meena S, Esther D, Vasanthi N. Survey on various data integrity attacks in cloud environment and the solutions. *IEEE Xplore*.

URL: https://ieeexplore.ieee.org/abstract/document/6528889/authors#authors (дата звернення: 15.04.2023).

26. Thapa, Suman, and Mailewa A. "The Role of Intrusion Detection/Prevention Systems in Modern Computer Networks: A Review." In Conference: *Midwest Instruction and Computing Symposium (MICS)*, 2020. vol. 53, pp. 1-14. (дата звернення: 14.05.2023).
27. Sudalai S. and S. S., A Survey on Cloud Security Issues and Challenges with Possible Measures *A Survey on Cloud Security Issues and Challenges with Possible Measures*. 2016. (дата звернення: 15.05.2023).
28. Centre for the Protection of National Infrastructure (CPNI). *Information Security Briefing* 01/2010: Cloud Computing. URL: http://www.cpni.gov.uk/Docs/cloud-computing-briefing.pdf (дата звернення: 19.04.2023).
29. Vodovatova, E. Cloud Security Risks & Threats in 2021, and How to Avoid Them. 2019. *The APP Solutions*.
    URL: https://theappsolutions.com/blog/development/cloud-security-risks/ (дата звернення: 19.04.2023).
30. Dedicated to the Belief That the Cloud Should Be Open – Open Cloud Manifesto. *Open Cloud Manifesto* 2009. URL: www.opencloudmanifesto.org/ (дата звернення: 19.04.2023).
31. Contributor, T., & Sales, F. (2021). compliance risk. *CIO*.
    URL: https://www.techtarget.com/searchcio/definition/compliance-risk (дата звернення: 19.04.2023).
32. Best Practices for Mitigating Risks in Virtualized Environments, Cloud Security Alliance – *Cloud Security Alliance*, 2015
    URL: https://downloads.cloudsecurityalliance.org/whitepapers/Best_Practices_for%
    20_Mitigating_Risks_Virtual_Environments_April2015_4-1-15_GLM5.pdf (дата звернення: 19.04.2023).

33. Azeez, N.; Odufuwa, O.; Misra, S.; Oluranti, J.; Damaševičius, R. Windows PE Malware Detection Using Ensemble Learning. *Informatics* 2021, *8*, 10. [Google Scholar] (дата звернення: 19.04.2023).
34. Toldinas, J.; Venčkauskas, A.; Damaševičius, R.; Grigaliūnas, Š.; Morkevičius, N.; Baranauskas, E. A Novel Approach for Network Intrusion Detection Using Multistage Deep Learning Image Recognition. *Electronics* 2021, *10*, 1854. [Google Scholar] (дата звернення: 19.04.2023).
35. Azeez, N.A.; Salaudeen, B.B.; Misra, S.; Damaševičius, R.; Maskeliunas, R. Identifying phishing attacks in communication networks using URL consistency features. *Int. J. Electron. Secur. Digit. Forensics* 2020, *12*, 200. [Google Scholar] (дата звернення: 19.04.2023).
36. Aid. Cloud Computing Attacks: A New Vector for Cyber Attacks. *Apriorit*. 2023. URL: https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks (дата звернення: 19.04.2023).
37. Damenu T. K. and Balakrishna C., "Cloud security risk management: A critical review," International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, pp. 370-375. (дата звернення: 15.05.2023).
38. Fray I. El, "A comparative study of risk assessment methods, MEHARI & CRAMM with a new formal model of risk assessment (FoMRA) in information systems," in *IFIP International Conference on Computer Information Systems and Industrial Management*, 2012, pp. 428-442:Springer (дата звернення: 15.05.2023).
39. ISO/IEC 27001:2022 and ISO/IEC 27002:2022. *IT Governance - Governance, Risk Management and Compliance for Information Technology*. URL: https://www.itgovernance.co.uk/iso27001-and-iso27002-2022-updates (дата звернення: 21.04.2023).

40. ISO/IEC-27005, Information Technology. Security Techniques. Information Security Risk Management: ISO/IEC 27005: 2022. *International Organization for Standardization*, 2022 (дата звернення: 15.05.2023).
41. Wangen G., Hallstensen C., and Snekkenes E., "A framework for estimating information security risk assessment method completeness," 2017, *Int. J. Inf. Secur.*, pp. 681–699. (дата звернення: 15.05.2023).
42. SP 800-30 Rev. 1, Guide for Conducting Risk Assessments | CSRC. *NIST Computer Security Resource Center | CSRC*. URL: https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final (дата звернення: 23.04.2023).
43. Labuschagne L., "A Framework for Comparing Different Information Security Risk Analysis Methodologies," Proceedings of SAICSIT, 2005, pp. 95–103, 2005. (дата звернення: 15.05.2023).
44. Caralli R. A., Stevens J. F., Young L. R., and Wilson W. R., "Introducing octave allegro: Improving the information security risk assessment process," *Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst*, 2007. (дата звернення: 15.05.2023).
45. Fransson C. and Laukka L., "Cloud risk analysis using OCTAVE Allegro: Identifying and analysing risks of a cloud service," Linköping University, 2021, pp. 1-42. (дата звернення: 15.05.2023).
46. Cramm. *ENISA*. URL: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html (дата звернення: 23.04.2023).
47. CRAMM Standard. CRAMM. – *CRAMM*. 2012. URL: www.CRAMM.com (дата звернення: 23.04.2023).
48. Sheikh J. and BhupendraMalviya, "Managing Cyber Risk and Security In Cloud Computing," International Journal of Advanced Computer Technology 2020, pp. 122-126. (дата звернення: 15.05.2023).

49. Lund M. S., Solhaug B., Stølen K., Model-Driven Risk Analysis: The CORAS Approach. Blindern: Springer, 2011. (дата звернення: 15.05.2023).
50. COBIT 2019 for Risk Management, *ISACA*. 2019 (дата звернення: 15.05.2023).
51. Franc G. COBIT 2019 - Review of the Framework and its Major Concepts. URL: https://www.linkedin.com/pulse/cobit-2019-review-framework-its-major-concepts-grégory-franc/ (дата звернення: 23.04.2023).
52. UcedaVelez, T., Morana, M.M.: Risk Centric Threat Modeling: process for attacksimulation and threat analysis. John Wiley & Sons 2015 (дата звернення: 15.05.2023).
53. Machine Learning Models for Secure Data Analytics: A taxonomy and threat model / R. Gupta et al. *Computer Communications*. 2020. Vol. 153. P. 406–440. URL: https://doi.org/10.1016/j.comcom.2020.02.008 (дата звернення: 23.04.2023).
54. Adopting threat modelling in agile software development projects / K. Bernsmed et al. *Journal of Systems and Software*. 2021. P. 111090. URL: https://doi.org/10.1016/j.jss.2021.111090 (дата звернення: 23.04.2023).
55. Xiong W., Lagerström R. Threat modeling – A systematic literature review. *Computers & Security*. 2019. Vol. 84. P. 53–69. URL: https://doi.org/10.1016/j.cose.2019.03.010 (дата звернення: 23.04.2023).
56. Brazhuk, A.: Security patterns based approach to automatically select mitigationsin ontology-driven threat modelling. 2020 (дата звернення: 23.04.2023).
57. K. Saatkamp et al. Application Threat Modeling and Automated VNF Selection for Mitigation using TOSCA *2019 International Conference on Networked Systems*, Munich, Germany, 18–21.03.2019. URL: https://doi.org/10.1109/netsys.2019.8854524 (дата звернення: 23.04.2023).

58. Pre-deployment Security Assessment for Cloud Services Through Semantic Reasoning / C. Cauli et al. *CAV 2021: Computer Aided Verification*, 20–23 July 2021. 2021. pp. 767–780.
59. Xiong, W., Hacks, S., Lagerstr¨om, R.: A method for quality assessment of threatmodeling languages: The case of enterpriselang. In: Barn, B., Sandkuhl, K., Asen-sio, E.S., Stirna, J. (eds.) Proceedings of the Forum at Practice of Enterprise Modeling 2021 (PoEM-Forum 2021), Riga, Latvia, November 24-26,2021. CEUR Workshop Proceedings, vol. 3045, pp. 49–58. CEUR-WS.org (дата звернення: 25.04.2023).
60. Threat modeling / K. Yskout та ін. *ICSE '20: 42nd International Conference on Software Engineering*, м. Seoul South Korea. New York, NY, USA, 2020. URL: https://doi.org/10.1145/3377816.3381741 (дата звернення: 25.04.2023).
61. Threat modelling cloud platform services by example: google cloud storage. *NCC Group Research Blog*. URL: https://research.nccgroup.com/2023/01/31/threat-modelling-cloud-platform-services-by-example-google-cloud-storage/ (дата звернення: 20.05.2023).
62. Manzoor S., Zhang H., Suri N. Threat Modeling and Analysis for the Cloud Ecosystem. *2018 IEEE International Conference on Cloud Engineering (IC2E)*, Orlando, FL, 17–20 April 2018. 2018. URL: https://doi.org/10.1109/ic2e.2018.00056 (дата звернення: 20.05.2023).
63. The STRIDE Threat Model - Satori. *Satori*. URL: https://satoricyber.com/glossary/the-stride-threat-model/ (дата звернення: 20.05.2023).
64. Kamatchi R., Ambekar K. Analyzing Impacts of Cloud Computing Threats in Attack based Classification Models. *Indian Journal of Science and Technology*. 2016. Vol. 9, no. 21. URL: https://doi.org/10.17485/ijst/2016/v9i21/95282 (дата звернення: 20.05.2023).

65. Аулов І. Ф. Дослідження моделі загроз ключових аспектів хмари та пропозиції захисту від них. *Східно-Європейський журнал провідних технологій*. 2015. № 77. (дата звернення: 20.05.2023).
66. Top Threats to Cloud Computing: Egregious Eleven Deep Dive | CSA. *CSA*. URL: https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/ (дата звернення: 21.05.2023).
67. Casey K., Bigelow S. J. What is shared responsibility model? – Definition from TechTarget.com. *Cloud Computing*. URL: https://www.techtarget.com/searchcloudcomputing/definition/shared-responsibility-model (дата звернення: 21.05.2023).

ДОДАТОК А

УДК 004.056.5

М. В. ЄСІНА, канд. техн. наук, А.А. КРАВЧЕНКО, С.О. КРАВЧЕНКО

ОГЛЯД ЗАГРОЗ БЕЗПЕЦІ ТА ЦІЛІСНОСТІ ДАНИХ У ХМАРНИХ ОБЧИСЛЕННЯХ

Вступ

Хмарні обчислення – це швидко набираюча популярності та розвитку технологія, яка поєднує у собі декілька підходів та моделей з надання та управління IT сервісами. Згідно з визначенням Національного інституту стандартів і технології (NIST) США, хмарні обчислення – це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), і, які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера [1]. Хмарні обчислення розглядаються як одна з найуспішніших обчислювальних технологій, здатних вирішити цілу низку проблем, що стоять перед людством.

Хмарні обчислення мають декілька ключових особливостей, як то надійність, широкий мережевий доступ, масштабованість інфраструктури, гнучкість, незалежність від місця розташування, економія на масштабах і економічна ефективність та стійкість [2, 3].

Через зростаючу популярність і широку експлуатацію послуг хмарних обчислень виникає необхідність високого рівня безпеки. У сьогоднішніх реаліях люди використовують технології хмарних обчислень у великих обсягах, наприклад, на роботі, в особистих цілях та інше, так як вони мають велику довіру до цих технологій. Щоб запобігти втраті довіреної інформації провайдери послуг мають забезпечити її цілісність.

Стаття присвячена огляду загроз безпеці та цілісності технологій хмарних обчислень, тому що це є важливим аспектом даної технології. Зазначимо, що безпека хмарних обчислень означає захист даних, тоді як цілісність – їх надійність. Безпека та цілісність даних є основною проблемою користувачів, пов'язаною із хмарними обчисленнями.

Основна частина

[4] визначає безпеку хмарних обчислень як «Піддомен комп'ютерної безпеки, мережевої безпеки та, ширше, інформаційної безпеки. Це стосується широкого набору політик, технологій і елементів керування, які застосовуються для захисту даних, додатків і відповідної інфраструктури хмарних обчислень».

Коли організація вирішує зберігати дані або розміщувати додатки в публічній хмарі, вона втрачає можливість мати фізичний доступ до серверів, на яких зберігається її інформація [8]. Як наслідок, потенційно конфіденційні дані піддаються ризику інсайдерських атак. Згідно зі звітом Альянсу хмарної безпеки за 2010 рік [5], внутрішні атаки є однією з семи найбільших загроз у хмарних обчисленнях. Тому постачальники хмарних послуг повинні забезпечити проведення регельних перевірок співробітників, які мають фізичний доступ до серверів у дата-центрі. Крім того, центри обробки даних рекомендується часто моніторити на предмет підозрілої активності. Існує чотири основні аспекти безпеки в хмарі, за які відповідають як постачальники, так і клієнти [6]:

- Обмеження доступу. Оскільки в хмарі всі ресурси доступні через Інтернет, дуже важливо переконатися, що лише належні користувачі матимуть доступ до потрібних їм інструментів протягом визначеного періоду часу.
- Захист даних. Організації повинні розуміти, де розташовано їхні ресурси, і застосувати відповідні елементи керування для захисту даних та інфраструктури, де вони розміщені.
- Відновлення даних. У разі порушення безпеки надзвичайно важливо мати надійне рішення для резервного копіювання даних і план їхнього відновлення.
- План реагування. У разі атак організацієм потрібен спеціальний план, який дасть їм змогу зменшити наслідки та запобігти ураженню інших систем.

Загрози цілісності

Як і у будь-якій іншій системі, загрози безпеки для технологій хмарних обчислень можна поділити на загрози конфіденційності, цілісності та доступності. Загалом цілісність даних означає захист даних від несанкціонованого видалення, модифікації чи фальсифікації [10].

Предметом дослідження цієї статті є саме загрози цілісності, які розглянуто нижче.

1) Несанкціонований доступ

Ця атака направлена на безконтрольні зміни даних, на які не зможе вплинати авторизований користувач. Зловмисник, який проводить несанкціонований доступ з послідовною зміною даних, може провести атаку ззовні або зсередини організації-власника хмари. Це найсерйозніша атака, якщо це станеться, то витік даних відбуватиметься шляхом використання старого обладнання та повторного використання драйверів [11].

2) Блокування даних

Ця загроза утворюється при переході від одного постачальника послуг до іншого. Так як різні постачальники надають різні послуги, тому при переході може трапитись втрата даних користувачів або їх блокування. У хмарі немає правил або умов щодо того, як зберігати дані, це залежить від постачальника хмарних послуг (CSP) [12]. Зазвичай, дані будуть розкидані по всьому серверу та системам. В ідеальній моделі міграція додатків від одного хмарного провайдера до іншого повинна бути простою, що є ще одним викликом для додатків хмарних обчислень, але оскільки кожен хмарний провайдер використовує окрему стандартну мову для своїх систем, це наразі неможливо.

3) SQL-ін'єкції

SQL-ін'єкції націлені на SQL-сервери, які запускають уразливі програми баз даних. Хакери використовують вразливі місця веб-серверів і вводять шкідливий код, щоб обійти вхід і отримати несанкціонований доступ до серверних баз даних. У разі успіху хакери можуть маніпулювати вмістом баз даних, отримати конфіденційні дані, віддалено виконувати системні команди або навіть взяти під контроль веб-сервер для подальшої злочинної діяльності [13].

4) Атака "людина посередині" (MiMA)

MiMA зазвичай виникає, коли різні користувачі хмари спілкуються один з одним або спільно використовують ресурси з хмарного середовища [14]. Недостатнє шифрування може зробити користувачів вразливими до атаки "людина посередині", яка є непрямою атакою [15]. TLS – криптографічний протокол, який дозволяє клієнт-серверному додатку [16] запобігти підслуховуванню будь-якої конфіденційної інформації, що відбувається на HTTPS, який використовує TLS. Якщо людина отримує доступ до невідомої мережі і виконує свою роботу в HTTP, зловмисник, який виступає в ролі посередника, потім скористається цим, перехопивши всі конфіденційні дані через HTTPS-пакети.

5) DDoS-атака

Мабуть,[l]у сучасних технологіях це є найбільш серйозною проблемою, оскільки не може бути усуненою повністю. На сьогоднішній момент є лише деякі методи пом'якшення наслідків, які допомагають зменшити ризики та послідовності таких атак. DDoS-атаки націлені на веб-сайти та сервери, порушуючи роботу мережевих сервісів з метою виснаження ресурсів програми. Зловмисники, які стоять за цими атаками, наводнюють сайт несанкціонованим трафіком, що призводить до погіршення функціональності сайту або взагалі виводить його з ладу [17].

6) Атаки на автентифікацію

Атаки на автентифікацію складно класифікувати як саме атаки на цілісність, але вони можуть спровокувати такі загрози, тому слід їх зазначити. Нижче наведено декілька відомих атак на автентифікацію.

- Атака на відтворення

Ця атака відбувається, коли невідома особа переглядає трафік даних, а потім надсилає комунікаційні дані на своє місце, як оригінального відправника. Щоб запобігти цій атаці, зазвичай впроваджують мітки часу та порядкові номери [18].

- Атака грубої сили або атака за словником

Це базова атака, при якій зловмисник перебирає всі можливі комбінації для пароля, щоб отримати доступ до даних користувачів. Чим більше довжина пароля, тим більше часу знадобиться зловмиснику, щоб вгадати правильний пароль [19].

- Фішингова атака

Йдеться про те, як зловмисник перебирає всі можливі способи атаки на жертву, підбираючи всі комбінації коду та паролів. Звон-таки, чим складніший код, тим більше часу знадобиться зловмиснику для його підбору [20], при цьому витрачений час буде зростати не лінійно.

7) Атака відкату

Такі атаки можуть виникати під час оновлення системи у випадку, якщо постачальник у цей момент надає старе програмне забезпечення для користування. Це може спровокувати втрату даних, що зберігаються у цій системі. Відкат також відбувається без належного видалення старих даних користувача та оновлення системи до нової версії [21].

8) Атака підробки тегів

Ця атака відбувається, якщо нечемний продавець обманює своїх клієнтів, показуючи неправильний штрих-код чи даючи неправильне посилання. Якщо користувач сканує його на своєму пристрої, то зловмисник отримує доступ до всіх конфіденційних даних, що призводить до можливих ризиків шахрайства та витоку приватної інформації [21].

9) Візантійська атака

Ця атака відбувається на різні частини хмарних обчислень шляхом зупинки або виходу з ладу систем. Це станеться, коли запит буде некоректно проходить через систему [21].

10) Атака на систему доменних імен (DNS)

Ця атака відбувається, якщо систему атакує якесь шкідливе програмне забезпечення. DNS перетворює доменні імена на IP-адреси, і користувач не може бачити, наскільки правильно відбувається перетворення. Кожного разу, коли відкривається невідома веб-сторінка, зловмисник може легко отримати доступ до персональної інформації, що використовується на серверах [22].

11) Сніфферні атаки

Атака відбувається коли користувач натискає на деякі SOAP (Simple Object Access Protocol) – повідомлення або шкідливе посилання. Після того, як натиснуте посилання буде активоване, програма перехоплює потік пакетів в мережі і отримує доступ до персональних даних користувачів, таких як паролі, реквізити банківських рахунків тощо, які не є зашифрованими [23]. Залежно від обсягу даних та їх характеру, внаслідок цієї атаки втрати даних можуть бути непомітними або стати причиною великих проблем для цілої організації.

Методи забезпечення цілісності даних у хмарному середовищі

Проаналізувавши наведені вище загрози, перейдемо до методів забезпечення цілісності та запобігання атак на цілісність у хмарних сховищах. Як було зазначено вище, не завжди можна повністю усунути загрози, але майже завжди можна прийняти міри для їх запобігання та зменшення ймовірних втрат. Існує декілька механізмів та схем, які було запропоновано для захисту володіння даними та їх цілісності в середовищі хмарних обчислень. Нижче наведено декілька механізмів та схем, які ми розглянуті в попередніх досліджених [21].

1. Пом'якшення наслідків підробки тегів та атак витоку даних

Щоб запобігти цій атаці, існує схема, запропонована Yun Zhu та ін. [24], відома як Cooperative Provable Data Possession (CPCP), яка використовується в поєднанні з двома іншими (Homomorphic Verifiable Response та Hash Index Hierarchy), що забезпечує прозору перевірку даних та надійний захист.

Сутність даного методу виглядає так: перед тим, як клієнт надсилає інформацію до CSP, він створює тег виклику, а потім надсилає його постачальнику хмарних послуг пізніше. Клієнт кидає виклик провайдеру хмарних послуг, перевіряючи цілісність даних за допомогою довіреної третьої сторони (TTP) [21].

2. Послаблення атаки відкату

У запропонованій схемі захист від атаки відкату в хмарному середовищі здійснюється шляхом застосування методу геш-дерева Меркла [25, 26]. У цьому методі тег блоку даних та значення його лічильника оновлюються щоразу, коли оновлюються нові дані. Якщо зловмисник хоче змінити дані, значення лічильника також зміниться.

3. Пом'якшення наслідків візантійського збою та зловмисних атак на дані

Рішенням для даної проблеми є запропонована Browers та ін. [27] криптосистема HAIL (High Availability and Integrity Layer) Protocol. Цей протокол гарантує, що дані користувача зберігаються неушкодженими і можуть бути безпечно отримані з серверів. Для забезпечення гарантії доступності даних використовується коригувальний код Erasure [21].

4. Захист цілісності даних за допомогою шифрування

Даний метод є найкращим для загального захисту даних у хмарному середовищі та використовується у будь-якій системі. Оскільки технології продовжують розвиватися, а старі технології стають вразливіше, з'являтимуться нові методи злому шифрів, а також фатальні недоліки в старих методах шифрування. Хмарні провайдери повинні постійно оновлювати своє шифрування, оскільки дані, які вони зазвичай містять, є особливо цінними [7]. Перед тим як зберігати дані на сервері, слід зашифрувати їх та обчислити геш-значення даних. Це гарантуватиме, що дані не були змінені [28].

5. Техніка доказового володіння даними (PDP)

Техніка PDP використовує протокол відповіді на запит для перевірки цілісності даних, що зберігаються на хмарному сервері. Цей метод використовує симетричне шифрування, наприклад, MAC або будь-яке інше. Файл заповнюється метаданими перед зберіганням або надсиланням його на хмарний сервер. Після надсилання файлу до постачальника хмарних послуг користувач все одно зберігає метадані файлу, щоб перевірити його цілісність. Після цього користувач видаляє локальну копію файлу та перевіряє докази володіння файлом сервером за допомогою протоколу відповіді на виклик [29].

6. Техніка доведення можливості вилучення (POR)

Метод Proof of Retrievability (POR) використовується для віддаленої перевірки даних, які зберігаються у постачальника хмарних послуг, за допомогою ключа автентифікації. У цьому методі дані не потрібно отримувати з CSP, і користувач також не зберігає оригінальну копію файлу локально. Користувач зберігає свій файл у CSP разом із ключем автентифікації. Потім користувач може перевіряти цілісність даних за допомогою ключа автентифікації, не отримуючи файл з CSP [29, 9].

Висновки

У цій статті було розглянуто поняття безпеки даних у хмарних обчисленнях та коротко оглянуто декілька з тих поширених загроз, що заважають забезпечити цілісність інформації, що там зберігається. Зараз технології хмарних обчислень – це те, чим люди користуються, майже не акцентуючи на це увагу, бо у сьогоденні це явище, що зустрічається майже усюди та у кожній компанії. Не дивлячись на те, що хмарні технології зазвичай впроваджують найсучасніші технології безпеки, на жаль, абсолютно позбутись усіх ризиків неможливо. Окрім огляду поширених загроз ця стаття оглядає можливі методи вирішення проблем, мінімізування можливих вразливостей від атак та забезпечення цілісності у хмарних обчисленнях.

Список літератури: 1. P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology,Vol.53,no.6, p. 50, 2009. 2. Reese, G. (2009) Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. Sebastopol, California: O'Reilly Media. 3. Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., and Brandic, I. (2009) Cloud computing and emerging IT platforms: Vision, hype, and reality for

delivering computing as the 5th utility. Future Generation Computer Systems, 25 (6), pp. 599-616. 4. Cloud computing security, Режим доступу – http://en.wikipedia.org/wiki/Cloud_ computing_security. 5. "Top Threats to Cloud Computing v1.0" Cloud Security Alliance. 6. Що таке безпека в хмарі?, Microsoft. Режим доступу – https://www.microsoft.com/uk-ua/security/business/security-101/what-is-cloud-security. 7. Rukavitsyn, Andrey N.; Borisenko, Konstantin A.; Holod, Ivan I.; Shorov, Andrey V. (2017). "The method of ensuring confidentiality and integrity data in cloud computing". *2017 XX IEEE International Conference on Soft Computing and Measurements (SCM)*. pp. 272–274. 8. Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu – Data Security and Privacy in Cloud Computing. 9. M. S. Giri, B. Gaur, and D. Tomar, A Survey on Data Integrity Techniques in Cloud Computing. 10. Yunchuan Sun, Junsheng Zhang zhangjs, Yongping Xiong, and Guangyu Zhu (2014) "Data Security and Privacy in Cloud Computing". 11. Dissanayaka, Akalanka Mailewa, Susan Mengel, Lisa Gittner, and Hafiz Khan. "Vulnerability prioritization, root cause analysis, and mitigation of secure data analytic framework implemented with mongodb on singularity linux containers." In Proceedings of the 2020 the 4th International Conference on Compute and Data Analysis, pp. 58-66. 2020. 12. A. Jyoti, M. Shrimali, S. Tiwari, and H. P. Singh, "Cloud computing using load balancing and service broker policy for IT service: a taxonomy and survey," J. Ambient Intell. Humaniz. Comput., vol. 11, no. 11, pp. 4785–4814, Nov. 2020, doi: 10.1007/s12652-020-01747-z. 13. Te-Shun Chou "Security threats on cloud computing vulnerabilities", International Journal of Computer Science & Information Technology (IJCSIT) Vol 5, No 3, June 2013, pp. 84-85. 14. Ramandeep Kaur, Pushpendra Kumar Pateriya, "A Study on Security Requirements in Different Cloud Frameworks", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013, pp.134-135. 15. Y. Chen, L. Li, and Z. Chen, "An Approach to Verifying Data Integrity for Cloud Storage," in 2017 13th International Conference on Computational Intelligence and Security (CIS), Dec. 2017, pp. 582–585, doi: 10.1109/CIS.2017.00135. 16. H. Mohapatra, "Handling of Man-In-The-Middle Attack in WSN Through Intrusion Detection System," Int. J. Emerg. Trends Eng. Res., vol. 8, no. 5, pp. 1503–1510, May 2020, doi: 10.30534/ijeter/2020/05852020. 17. What is a DDoS attack? Режим доступу – https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack. 18. Lai, Cheng-I., Alberto Abad, Korin Richmond, Junichi Yamagishi, NajimDehak, and Simon King. "Attentive filtering networks for audio replay attack detection." In ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp. 6316-6320. IEEE, 2019. 19. Shetty, Roshan Ramprasad, Akalanka Mailewa Dissanayaka, Susan Mengel, Lisa Gittner, Ravi Vadapalli, and Hafiz Khan. "Secure NoSQL based medical data processing and retrieval: the exposome project." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 99-105. 2017. 20. Mailewa Dissanayaka, Akalanka, Roshan Ramprasad Shetty, Samip Kothari, Susan Mengel, Lisa Gittner, and Ravi Vadapalli. "A review of MongoDB and singularity container security in regards to hipaa regulations." In Companion Proceedings of the10th International Conference on Utility and Cloud Computing, pp. 91-97. 2017. 21. "Survey on various data integrity attacks in cloud environment and the solutions - IEEE Conference Publication." Режим доступу – https://ieeexplore.ieee.org/abstract/document/6528889. 22. Thapa, Suman, and Akalanka Mailewa. "The Role of Intrusion Detection/Prevention Systems in Modern Computer Networks: A Review." In Conference: Midwest Instruction and Computing Symposium (MICS), vol. 53, pp. 1-14. 2020. 23. S. Sudalai and S. S., A Survey on Cloud Security Issues and Challenges with Possible MeasuresA Survey on Cloud Security Issues and Challenges with Possible Measures. 2016. 24. Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231–2244, Dec. 2012, doi: 10.1109/TPDS.2012.66. 25. J. Feng, Y. Chen, D. H. Summerville, and K. Hwang, "Fair Non-repudiation Framework for Cloud Storage: Part II," in Cloud Computing for Enterprise Architectures, Z. Mahmood and R. Hill, Eds. London: Springer, 2011, pp. 283–300. 26. J. Feng, Y. Chen, D. Summerville, W. Ku, and Z. Su, "Enhancing cloud storage security against roll-back attacks with a new fair multi-party nonrepudiation protocol," in 2011 IEEE Consumer Communications and Networking Conference (CCNC), Jan. 2011, pp. 521–522, doi: 10.1109/CCNC.2011.5766528. 27. H. Lin and W. Tzeng, "A Secure Erasure Code-Based Cloud Storage System with Secure Data Forwarding," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 6, pp. 995–1003, Jun. 2012, doi: 10.1109/TPDS.2011.252. 28. R. V. Rao and K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing," Procedia Comput. Sci., vol. 48, pp. 204–209, Jan.2015, doi: 10.1016/j.procs.2015.04.171. 29. K. N. Sevis and E. Seker, "Survey on Data Integrity in Cloud," in 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Jun. 2016, pp. 167–171, doi: 10.1109/CSCloud.2016.35.

ДОДАТОК Б

ЗАГРОЗИ ЦІЛІСНОСТІ ДАНИХ ТА ПРОПОНОВАНІ РІШЕННЯ У ХМАРНИХ ОБЧИСЛЕННЯХ

Анастасія КРАВЧЕНКО*, Софія КРАВЧЕНКО*, Всеволод БОБУХ°

* Харківський національний університет імені В. Н. Каразіна, майдан Свободи 4, Харків, Україна
° АТ «Інститут інформаційних технологій», вул. Колегіальна 15, Харків, Україна

Анотація. *Зараз технології хмарних обчислень – це те, чим люди користуються майже усюди. Хмарні технології зазвичай впроваджують найсучасніші технології безпеки, але абсолютно позбутись усіх ризиків неможливо, а враховуючи той факт, що люди довіряють важливу інформацію, треба максимально забезпечити її цілісність.*

Ключові слова. *Хмарні обчислення, цілісність, загрози цілісності.*

1. Вступ

Хмарні обчислення розглядаються як одна з найуспішніших обчислювальних технологій, здатних вирішити цілу низку проблем, що стоять перед людством. Згідно з визначенням NIST США, хмарні обчислення – це модель забезпечення повсюдного та зручного доступу на вимогу, через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню, і, які можуть бути оперативно надані та звільнені з мінімальними управлінськими затратами та зверненнями до провайдера [1]. Хмарні обчислення мають декілька ключових особливостей, як надійність, широкий мережевий доступ, масштабованість інфраструктури, гнучкість, незалежність від місця розташування, економія на масштабах і економічна ефективність та стійкість [2].

2. Забезпечення цілісності в хмарних обчисленнях

Безпека хмарних обчислень визначається як «Піддомен комп'ютерної безпеки, мережевої безпеки та, ширше, інформаційної безпеки. Це стосується широкого набору політик, технологій і елементів керування, які застосовуються для захисту даних, додатків і відповідної інфраструктури хмарних обчислень».

Коли організація вирішує зберігати дані або розміщувати додатки в публічній хмарі, вона втрачає можливість мати фізичний доступ до серверів, на яких зберігається її інформація [4] .Як наслідок, потенційно конфіденційні дані піддаються ризику інсайдерських атак. Крім того, центри обробки даних рекомендується часто перевіряти на предмет підозрілої активності.

2.1. Поширені атаки на цілісність

Цілісність даних означає захист даних від несанкціонованого видалення, модифікації чи фальсифікації [5].

1. Несанкціонований доступ. Атака направлена на безконтрольні зміни даних, на які не зможе впливати авторизований користувач.

2. Блокування даних. Загроза утворюється при переході від одного постачальника послуг до іншого і так як різні постачальники надають різні послуги, тому при переході може трапитись втрата даних користувачів або їх блокування.

3. SQL-ін'єкції. Атака націлена на SQL-сервери, які запускають уразливі програми баз даних. Хакери використовують вразливі місця веб-серверів і вводять шкідливий код, щоб обійти вхід і отримати несанкціонований доступ до серверних баз даних.

4. Атака "людина посередині" (MiMA). MiMA зазвичай виникає, коли різні користувачі хмари спілкуються один з одним або спільно використовують ресурси з хмарного середовища [5]. Недостатнє шифрування може зробити користувачів вразливими до атаки MiMA, яка є непрямою атакою.

5. DdoS-атака. DDoS-атаки націлені на веб-сайти та сервери, порушуючи роботу мережевих сервісів з метою виснаження ресурсів програми.

6. Атака підробки тегів. Атака відбувається, якщо продавець обманює своїх клієнтів, показуючи неправильний штрих-код, за яким переходить користувач та втрачає контроль над безпекою особистих даних.

7. Візантійська атака. Ця атака відбувається на різні частини хмарних обчислень шляхом зупинки або виходу з ладу систем.

2.2. Методи забезпечення цілісності даних

Проаналізувавши наведені вище загрози, перейдемо до методів забезпечення цілісності та запобігання атак на цілісність у хмарних сховищах. Нижче наведено декілька механізмів, що використовують для захисту володіння даними та їх цілісності в середовищі хмарних обчислень.

1. Пом'якшення наслідків підробки тегів та атак витоку даних. Щоб запобігти цій атаці, існує схема, запропонована Yun Zhu та ін. [4]. Сутність методу: перед тим, як клієнт надсилає інформацію до CSP, він створює тег виклику, надсилає його постачальнику хмарних послуг. Клієнт кидає виклик провайдеру, перевіряючи цілісність даних за допомогою TTP.

2. Послаблення атаки відкату. У цьому методі тег блоку даних та значення його лічильника оновлюються щоразу, коли оновлюються нові дані.

3. Пом'якшення наслідків візантійського збою та зловмисних атак на дані. Рішенням для даної проблеми є криптосистема HAIL Protocol, який гарантує, що дані користувача зберігаються неушкодженими і можуть бути безпечно отримані з серверів.

4. Захист цілісності даних за допомогою шифрування. Даний метод є найбільш поширеним. Хмарні провайдери повинні постійно оновлювати своє шифрування, оскільки дані, які вони зазвичай містять, є особливо цінними. Перед тим як зберігати дані на сервері, слід зашифрувати їх та обчислити геш-значення даних.

5. Техніка доказового володіння даними (PDP). Техніка PDP використовує протокол відповіді на запит для перевірки цілісності даних, що зберігаються на хмарному сервері. Файл заповнюється метаданими перед зберіганням або надсиланням його на хмарний сервер. Після надсилання файлу до постачальника хмарних послуг користувач все одно зберігає метадані файлу, щоб перевірити його цілісність. Після цього користувач видаляє локальну копію файлу та перевіряє докази володіння файлом сервером за допомогою протоколу відповіді на виклик [4].

6. Техніка доведення можливості вилучення (POR). Метод POR використовується для віддаленої перевірки даних, які зберігаються у постачальника хмарних послуг, за допомогою ключа автентифікації. Користувач зберігає свій файл у CSP разом із ключем автентифікації. Потім користувач може перевірити цілісність даних за допомогою ключа автентифікації, не отримуючи файл з CSP [3].

3. Висновки

У цій роботі було коротко оглянуто декілька з тих поширених загроз, що заважають забезпечити цілісність інформації, що там зберігається та методи їх запобігання. На жаль, повністю забезпечити це не завжди можливо, але можна мінімізувати ризики, і саме на такі методи було звернено увагу.

4. Список літератури

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," National Institute of Standards and Technology,Vol.53,no.6, p. 50, 2009.

[2] Reese, G. (2009) Cloud Application Architectures: Building Applications and Infrastructure in the Cloud. Sebastopol, California: O'Reilly Media.

[3] K. N. Sevis and E. Seker, "Survey on Data Integrity in Cloud," in 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), Jun. 2016, pp. 167–171.

[4] Yunchuan Sun, Junsheng Zhang, Yongping Xiong, and Guangyu Zhu – Data Security and Privacy in Cloud Computing.

[5] Ramandeep Kaur, Pushpendra Kumar Pateriya, "A Study on Security Requirements in Different Cloud Frameworks", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-1, March 2013, pp.134-135.