**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» травня 2024 р.

# ПОЯСНЮВАЛЬНА ЗАПИСКА

## кваліфікаційної роботи

**галузь знань** *12 Інформаційні технології*
(шифр і назва галузі знань)
**спеціальність** *125 Кібербезпека*
(код і назва спеціальності)
**освітній ступень** *магістр*
**освітньо-наукова програма** *Кібербезпека*
(назва освітньої програми)

**на тему:** «Засоби та механізми захисту інформації у хмарному середовищі»

**Виконавець:** студент ІІ курсу, групи КБм-22

_____ **Іван БЕРЕГОВИЙ**
(підпис) (Ім'я, ПРІЗВИЩЕ)

| | **Ім'я, ПРІЗВИЩЕ** | **Підпис** |
|---|---|---|
| **Науковий керівник** | Лариса МИРУТЕНКО | |
| **Нормоконтроль** | Сергій ДАКОВ | |

**Київ 2024**

**Міністерство освіти і науки України**
**Київський національний університет імені Тараса Шевченка**

**Факультет інформаційних технологій**
**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**
В.о. завідувача кафедри
кібербезпеки
та захисту інформації
_____ Іван ПАРХОМЕНКО
«17» листопада 2023 р.

# ЗАВДАННЯ
## на виконання кваліфікаційної роботи

**спеціальності** *125 Кібербезпека*
(код і назва спеціальності)

**освітній ступень** *магістр*

**Здобувача(ки)** КБм-22 (група) Берегового Івана Геннадійовича (прізвище ім'я по-батькові)

**Тема кваліфікаційної роботи** Засоби та механізми захисту інформації у хмарному середовищі

### 1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол № 5 від 15.11.2023 р.

### 2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

| | |
|---|---|
| **Об'єкт досліджень** | Процес захисту інформації хмарного середовища. |
| **Предмет досліджень** | Засоби та механізми захисту інформації в хмарному середовищі. |
| **Мета** | Забезпечення безпеки хмарного середовища з використанням засобів та механізмів захисту. |

| | |
|---|---|
| **Вихідні дані для проведення роботи** | Моделі надання хмарних сервісів, міжнародні стандарти, регламенти, віртуальне середовище, хмарні провайдери, засоби мережевого захисту. |

## 3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

| | |
|---|---|
| **Наукова новизна** | удосконалення засобів та механізмів, які включають стратегії захисту інформації в хмарному середовищі від кібератак |
| **Практична цінність** | забезпечення захисту інформаційних ресурсів хмарних середовищ поєднуючи засоби та механізми захисту, які спираються на стратегії активної протидії. |

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота виконана у повному обсязі відповідно до теми.

## 5. ЕТАПИ ВИКОНАННЯ РОБОТИ

| **Найменування етапів робіт** | **Строки виконання робіт (початок-кінець)** |
|---|---|
| Уточнення постановки задачі | 17.11.2023 – 26.11.2023 |
| Аналіз літературних джерел | 27.11.2023 – 24.12.2023 |
| Ознайомлення з сучасними трактуваннями хмарних технологій | 25.12.2023 – 14.01.2024 |
| Розгляд нормативно-правових актів, регулюючих функціонування та захист інформації в хмарних технологіях | 15.01.2024 – 28.01.2024 |
| Дослідження загроз, вразливостей та атак, що спрямовуються на хмарні середовища | 29.01.2024 – 11.02.2024 |
| Аналіз рекомендацій стосовно уникнення можливих загроз від хмарних провайдерів та експертів | 12.02.2024 – 18.02.2024 |
| Дослідження існуючих заходів та засобів з забезпечення інформаційної безпеки в хмарних середовищ | 19.02.2024 – 25.02.2024 |
| Ознайомлення з існуючими стратегіями активної протидії мережевим атакам | 26.02.2024 – 03.03.2024 |
| Розгляд відомих хмарних провайдерів | 04.03.2024 – 10.03.2024 |
| Налаштування інформаційної безпеки в AWS | 11.03.2024 – 24.03.2024 |

| Найменування етапів робіт | Строки виконання робіт (початок-кінець) |
|---|---|
| Розробка рекомендацій щодо захисту інформаційних ресурсів для хмарного середовища | 25.03.2024 – 07.04.2024 |
| Побудова концепта засобу та його механізмів активної протидії | 08.04.2024 – 05.05.2024 |
| Оформлення пояснювальної записки згідно методичних рекомендацій | 06.05.2024 – 12.05.2024 |
| Подача пакету документів на розгляд ЕК | 13.05.2024 – 17.05.2024 |

## 6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економічний ефект** Зменшення витрат на захист інформації у хмарному середовищі та створення нових ринків продуктів та послуг у сфері кібербезпеки хмарних середовищ.

**Соціальний ефект** Створення нових робочих місць у сфері кібербезпеки хмарних середовищ, підвищення кіберграмотності населення та збільшення загального рівня безпеки та захищеності інформації в суспільстві.

## 7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ Лариса МИРУТЕНКО
(підпис) (Ім'я, ПРІЗВИЩЕ)

Завдання прийняв до виконання _____ Іван БЕРЕГОВИЙ
(підпис) (Ім'я, ПРІЗВИЩЕ)

Дата видачі завдання: 17.11.2023 р.
Термін подання кваліфікаційної роботи до ЕК 17.05.2024 р.

# РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Засоби та механізми захисту інформації у хмарному середовищі» складається зі списку скорочень, вступу, основної частини, що містить 4 розділи, висновків і списку використаних джерел. Загальний обсяг роботи – 93 сторінки. Робота містить 19 рисунків, 5 таблиць. Кількість використаних літературних джерел включає 57 найменувань.

Об’єктом дослідження є процес захисту інформації хмарного середовища.

Мета роботи – забезпечення безпеки хмарного середовища з використанням засобів та механізмів захисту.

Предмет дослідження – засоби та механізми захисту інформації в хмарних середовищах.

Метод дослідження – дослідження, аналіз та визначення принципів функціонування хмарних середовищ, їх сервісів та вразливостей, що можуть вплинути на них.

В роботі проведено аналіз функціональних особливостей існуючих хмарних середовищ, типових загроз та способів їх протидії.

Розроблено рекомендації стосовно побудови й застосування механізмів і засобів захисту інформаційної безпеки в хмарному середовищі.

Практичне значення роботи полягає у забезпеченні захисту інформаційних ресурсів хмарних середовищ поєднуючи засоби та механізми захисту, які спираються на стратегії активної протидії.

Наукова новизна даної роботи полягає у вдосконаленні засобів та механізмів, які включають стратегії захисту інформації в хмарному середовищі від кібератак.

Результати здійснених у дипломній роботі досліджень можуть бути використані спеціалістами із захисту в сфері хмарних технологій.

Напрямки подальших досліджень: побудова засобів та механізмів інформаційної безпеки для хмарних середовищ.

Ключові слова: хмарні технології, хмарні середовища, безпека, загроза, хмарні сервіси, хмарні провайдери, засоби захисту, Amazon AWS.

# ЗМІСТ

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

| | | |
|---|---|---|
| AES | - | Advanced Encryption Standard; |
| API | - | Application Programming Interface; |
| ARP | - | Address Resolution Protocol; |
| AWS | - | Amazon Web Services; |
| CASB | - | Cloud Access Security Broker; |
| CDN | - | Content Delivery Network; |
| CSA | - | Cloud Security Alliance; |
| CSP | - | Content Security Policy; |
| CSPM | - | Cloud Security Posture Management; |
| CSRF | - | Cross-Site Request Forgery; |
| CWPP | - | Cloud Workload Protection Platforms; |
| DDoS-атака | - | Distributed Denial of Service; |
| DLP | - | Data Loss Prevention; |
| DNS | - | Domain Name System; |
| DoS-атака | - | Denial of Service; |
| ENISA | - | European Union Agency for Network and Information Security; |
| GCP | - | Google Cloud Platform; |
| GDPR | - | General Data Protection Regulation; |
| HIPAA | - | Health Insurance Portability and Accountability Act; |
| HTTP | - | HyperText Transfer Protocol; |
| IaaS | - | Infrastructure as a Service; |
| IAM | - | Identity and Access Management; |
| IDE | - | Integrated Development Environment; |
| IDS | - | Intrusion Detection System; |
| IP-адреса | - | Internet Protocol Address; |
| IPS | - | Intrusion Prevention System; |
| ISO | - | International Organization for Standardization; |

| | | |
|---|---|---|
| MitM-атака | - | Man-in-the-Middle; |
| NIST | - | National Institute of Standards and Technology; |
| NLP | - | Natural Language Processing; |
| ORM | - | Object-Relational Mapping; |
| PaaS | - | Platform as a Service; |
| PCI DSS | - | Payment Card Industry Data Security Standard; |
| RBAC | - | Role-Based Access Control; |
| SaaS | - | Software as a Service; |
| SDK | - | Software Development Kit; |
| SIEM | - | Security Information and Event Management; |
| SIM | - | Security Information Management; |
| SOAR | - | Security Orchestration, Automation, and Response; |
| SWG | - | Secure Web Gateways; |
| TCP | - | Transmission Control Protocol; |
| TDR | - | Threat Detection and Response; |
| VPN | - | Virtual Private Network; |
| WAF | - | Web Application Firewall; |
| XSS-атака | - | Cross Site Scripting; |
| ЄС | - | Європейський Союз; |
| ІБ | - | інформаційна безпека; |
| ІТ | - | інформаційні технології; |
| ІКС | - | інформаційно-комунікаційні системи; |
| НСД | - | несанкціонований доступ; |
| ОС | - | операційна система; |
| ПЗ | - | програмне забезпечення; |
| ПК | - | персональний комп’ютер; |
| ШІ | - | штучний інтелект. |

# ВСТУП

Ми живемо у 21-му столітті. У віці технологічного прогресу, коли щодня винаходять щось нове. Коли щодня з'являються нові різні сервіси. Коли зберігати інформацію в Інтернеті вважається однією з зручних і безпечних функцій. Все це призвело до того, що більшість людей та організацій почали зберігати інформацію в електронному вигляді. Таким чином, «хмара» є сьогодні одним з провідних трендів світового ринку інформаційних технологій.

Дана тенденція полягає в тому, що сучасні компанії активно залежать від обробки даних і витрат на управління своїми обчислювальними ресурсами. Річні витрати на це невпинно зростають, оскільки підприємства інвестують значні кошти у програмне забезпечення, комп'ютерну техніку та телекомунікаційне обладнання. Хмарні обчислення пропонують концепцію, яка спрямована на звільнення організацій та їх персоналу від додаткових витрат на IT.

Хмарні технології надають користувачам можливість зберігати, обробляти та обмінюватися даними через мережу Інтернет, використовуючи віртуальні обчислювальні ресурси, що знаходяться на віддалених серверах. Завдяки їм користувачам доступні різноманітні сервіси, такі як зберігання даних, обчислювальні потужності та програмне забезпечення, які вони можуть використовувати за необхідності, не потребуючи власних фізичних серверів чи інфраструктури.

Видатні аналітики передбачають значний попит на хмарні технології і вражаюче зростання доходів для компаній, що надають хмарні сервіси.

Однак разом зі зростанням популярності хмарних технологій збільшується й обсяг загроз для безпеки даних у цих середовищах. Зловмисники постійно шукають нові способи використання вразливостей в хмарних сервісах для несанкціонованого доступу до інформації, викрадення даних, введення у систему шкідливого коду та інших злочинних дій. Вимоги до безпеки стають важливим

фактором при вирішенні питання про використання інформаційно-технічних послуг, зокрема, щодо переходу до публічних хмарних обчислень.

Способи захисту інформації постійно змінюються, оскільки суспільство та технології розвиваються. Це породжує потребу у вдосконаленні захисту інформації. Основне питання полягає в тому, чи забезпечується достатній рівень захисту персональних даних у різних сервісах, зокрема, у хмарних технологіях, у сучасних умовах?

Отже, забезпечення безпеки інформації у хмарному середовищі стає вельми актуальним завданням. Від країни, яка має намір використовувати хмарні сервіси, вимагається належний рівень обізнаності з методами захисту даних та вміння правильно вибирати та налаштовувати засоби безпеки. У цьому контексті виникає необхідність у вивченні та розробці ефективних засобів та механізмів захисту інформації у хмарних середовищах, щоб забезпечити конфіденційність, цілісність та доступність даних для користувачів.

Метою даної кваліфікаційної роботи є забезпечення безпеки хмарного середовища з використанням засобів та механізмів захисту.

Для досягнення зазначеної мети поставлені наступні завдання:

- аналіз теоретичних відомостей про хмарні технології;
- аналіз нормативно-правової бази у сфері інформаційної та кібербезпеки в «хмарах»;
- аналіз сучасних загроз та вразливостей інформаційної безпеки у хмарному середовищі;
- визначення основних загроз інформаційним ресурсам при використанні хмарних технологій;
- дослідження доступних інструментів та технологій захисту даних у хмарних системах;
- визначення найефективніших стратегій захисту інформації в хмарному середовищі;
- конфігурація хмарних сервісів для забезпечення інформаційної безпеки;

- формування рекомендацій щодо основних засобів та механізмів захисту на прикладі хмарного середовища.

Об’єктом дослідження є процес захисту інформації хмарного середовища.

Предмет дослідження – засоби та механізми захисту інформації в хмарному середовищі.

Метод дослідження – дослідження, аналіз та визначення принципів функціонування хмарних середовищ, їх сервісів та вразливостей, що можуть вплинути на них.

Практична цінність дипломної роботи полягає у забезпеченні захисту інформаційних ресурсів хмарних середовищ поєднуючи засоби та механізми захисту, які спираються на стратегії активної протидії.

Науковою новизною даної роботи є удосконалення засобів та механізмів, які включають стратегії захисту інформації в хмарному середовищі від кібератак.

# РОЗДІЛ 1
# ХМАРНІ ТЕХНОЛОГІЇ В ЦИФРОВОМУ ПРОСТОРІ

## 1.1 Характеристика хмарних технологій та їх класифікація

Не секрет, що хмарні технології зараз знаходяться на хвилі популярності: економічність, легкість розгортання, розрахована на багато користувачів архітектура – все це сприяє швидкому поширенню хмар і захопленню ними більшої частини ринку інформаційних технологій. На сьогоднішній день економічність хмар робить їх особливо популярними для зберігання різної інформації.

Сучасні інтернет-технології стали доступними і займають важливе місце практично у всіх галузях людської діяльності, включаючи освіту. Маючи досвід розвинених зарубіжних країн, відмінним рішенням для оптимізації навчального процесу є хмарні технології, доступ до яких здійснюється через мережу Інтернет [1].

Основний принцип хмарних технологій полягає в тому, що інформація зберігається та обробляється засобами веб-сервера, а результат даних обчислень надається користувачеві за допомогою веб-браузера. Користувачі отримують можливість створювати та редагувати текстові документи, математичні таблиці, прості векторні зображення, редагувати графічні файли, створювати та демонструвати комп’ютерні презентації, використовувати дисковий простір провайдера для зберігання резервних копій даних [2].

Однією з необхідних умов переходу до використання хмарних технологій є модернізація інформаційно-телекомунікаційної інфраструктури, зазвичай прихованої від користувача [3].

Технології хмарних обчислень дозволяють уникати прив’язки фізичних серверів до конкретних програм та окремих користувачів. Працюючи у хмарі, користувач вибирає ті програми, які необхідні для роботи [4].

В наш час термін «хмара» стає все більш популярним у світі інформаційних технологій. Терміни, такі як «хмарний сервер», «хмарні послуги», «хмарна безпека» та інші, зустрічаються дуже часто. Хмарні технології швидко поширюються, задовольняючи потреби сучасного світу. Суттєве зростання витрат на створення та управління інформаційними системами, а також загрози інформаційної безпеки, змушують багатьох керівників шукати нові методи підвищення ефективності в інформаційній сфері підприємств і організацій. Перехід до хмарних технологій є одним з сучасних шляхів досягнення цієї мети.

Хмарні обчислення, або cloud computing, відносяться до надання користувачеві комп'ютерних ресурсів та потужностей через Інтернет-сервіс. У такому форматі обчислювальні ресурси надаються користувачеві у «чистому» вигляді, при цьому він може не мати уявлення про те, які саме комп'ютери обробляють його запити або під якою операційною системою це відбувається. Ця технологія ґрунтується на принципах розподіленої обробки даних і забезпечує користувачеві віддалений доступ до наданих у хмарі послуг.

Термін «хмарні обчислення» відноситься до набору різноманітних сервісів, до яких можна отримати доступ через Інтернет. Це потужне рішення, яке дозволяє вирішувати доволі складні завдання.

Програми запускаються та надають результати своєї роботи у вікно стандартного веб-браузера на локальному ПК. При цьому всі необхідні для роботи додатки та їх дані знаходяться на віддаленому сервері в Інтернеті. Комп'ютери, які використовуються для проведення хмарних обчислень, називаються обчислювальною хмарою. При цьому навантаження між комп'ютерами, які утворюють обчислювальну хмару, розподіляється автоматично.

Але, на жаль, хмарні послуги також становлять підвищені ризики та більш обмежену можливість контролю. Саме в цьому полягають головні проблеми хмарних технологій.

Один з ключових підходів до реалізації обчислювальної інфраструктури – це технологія віртуалізації. Вона полягає в наданні набору обчислювальних ресурсів або їх логічного об’єднання, що абстраговані від фізичної реалізації. При цьому забезпечується логічна ізоляція обчислювальних процесів, які виконуються на одному фізичному ресурсі (хості). Сукупність комп’ютерних ресурсів, які емулюють роботу окремих компонентів апаратного або програмного забезпечення, або навіть цілої комп’ютерної техніки, називається віртуальною машиною. Можливість існування декількох віртуальних машин на одному реальному комп’ютері дозволяє незалежно працювати з декількома операційними системами та програмами на одному фізичному сервері (вузлі).

В даний час існує дві основні технології створення систем обчислень, що базуються на сервері віртуалізації [5]:

1. Віртуалізація на основі гіпервізора: в цьому підході, віртуалізація здійснюється за допомогою гіпервізора - програми або апаратній схемі в комп'ютерах, що забезпечує або дозволяє одночасне, паралельне виконання декількох або навіть багатьох операційних систем на одному і тому ж хост-комп'ютері. Гіпервізор також забезпечує ізоляцію операційних систем одна від одної, захист і безпеку, поділ ресурсів між різними запущеними ОС і управління ресурсами. Прикладами хмарних технологій на основі гіпервізора є рішення Amazon, Azure, VMWare.

2. Контейнерна віртуалізація: підхід з використанням такої віртуалізації дозволяє запускати в хмарі операційні системи будь-яких виробників, але втрачаючи при цьому в продуктивності від 8 до 12 відсотків в порівнянні з використанням фізичного сервера. Цей підхід вигідніший з точки зору обчислювальної продуктивності системи і економії дискових ресурсів, так як контейнери використовують ядро основної системи. При цьому користувачі обмежені у виборі операційної системи тільки збірками сімейства GNU/Linux, що в більшості випадків розглядається як істотний недолік контейнерної віртуалізації. У той же час, суттєва перевага в продуктивності дозволяє в цьому випадку використовувати ресурси хмари навіть для високопродуктивних

обчислень. В останні роки і такі великі гравці на ринку хмарних послуг, як Amazone і Azure, крім традиційної віртуалізації на основі гіпервізора стали надавати послуги на основі контейнерних технологій. Google використовували дану технологію з самого початку як основну.

Національним інститутом стандартів і технологій США встановлені такі обов'язкові характеристики хмарних обчислень [6]:

1. Самообслуговування на вимогу (On-demand self-service). У споживача є можливість отримати доступ до наданих обчислювальних ресурсів в односторонньому порядку в разі потреби, автоматично, без необхідності взаємодії з співробітниками кожного постачальника послуг.

2. Широкий мережевий доступ (Broad network access). Надані обчислювальні ресурси доступні по мережі через стандартні механізми для різних платформ, тонких і товстих клієнтів (мобільних телефонів, планшетів, ноутбуків, робочих станцій та інше).

3. Об'єднання ресурсів в пули (Resource pooling). Обчислювальні ресурси провайдера об'єднуються в пули для обслуговування багатьох споживачів за мультитенантної (multi-tenant) моделі. Пули включають в себе різні фізичні та віртуальні ресурси, які можуть бути динамічно призначені і перепризначені згідно з запитами споживачів. Немає необхідності в тому, щоб споживач знав точне місце розташування ресурсів, проте можна зазначити їх місцезнаходження на більш високому рівні абстракції (наприклад, країна, регіон або центр обробки даних). Прикладами такого роду ресурсів можуть бути системи зберігання, обчислювальні потужності, пам'ять, пропускна здатність мережі.

4. Миттєва еластичність (Rapid elasticity). Ресурси можуть бути еластично виділені і звільнені, в деяких випадках автоматично, для швидкого масштабування пропорційно до попиту. Для споживача можливості надання ресурсів зображаються як необмежені, тобто вони можуть бути присвоєні в будь-якій кількості і в будь-який час.

5. Вимірюваний сервіс (Measured service). Хмарні системи автоматично керують і оптимізують ресурси за допомогою засобів вимірювання, реалізованих

на рівні абстракції стосовно різного роду сервісів (наприклад, керування зовнішньою пам'яттю, обробкою, пропускною здатністю або активними призначеними для користувача сесіями. Використані ресурси можна відстежувати і контролювати, що забезпечує прозорість як для постачальника, так і для споживача, що використовує сервіс.

### 1.2 Моделі надання хмарних сервісів

У своїй спеціальній публікації за номером SP800-144 Національний інститут стандартів і технологій США (National Institute of Standards and Technology, NIST) визначає три моделі хмарних сервісів наступним чином [7]:

1. SaaS: програмне забезпечення як послуга

SaaS (Software-as-a-Service) використовує мережу Інтернет для доставки додатків, які управляються сторонніми постачальниками і чий інтерфейс доступний клієнтській стороні. Більшість SaaS додатків можна запускати безпосередньо з веб-браузера, без необхідності завантаження або попередньої установки. SaaS позбавляє від необхідності встановлювати і запускати додатки на персональних комп'ютерах. З використанням SaaS, спрощується задача підприємств з раціоаналізації технічного обслуговування і підтримки, тому що в послуги постачальника входить обслуговування: додатків, часу виконання, даних, проміжного програмного забезпечення, операційних систем, віртуалізації серверів, сховищ і мережі. Gmail є одним з відомим прикладів поштового оператора SaaS.

У різних сервісах клієнтом контролюються різні аспекти безпеки незалежно від провайдера.

У моделі SaaS як платформа, так і інфраструктура повністю управляється провайдером хмарних послуг. Це означає, що, якщо операційна система або сервіс не налаштовані належним чином, то дані на більш високому прикладному рівні можуть бути в небезпеці. Для покупців у цьому випадку не обов'язково знати, як надаються ці послуги, які включають в себе: мережу, сервери,

операційні системи, сховища і навіть окремі функції додатків. Користувачеві важливо, щоб сервіс був досить дешевий і доступний в будь-який час, коли він необхідний. Тому багато деталей функціонування сервісу і його інфраструктура виявляються прихованими для користувача. У можливостях управління клієнт виявляється обмеженим тільки мінімальним набором налаштувань конфігурації програми під свої потреби. Salesforce.com, Google є одними з найвідоміших провайдерів SaaS послуг.

2. PaaS: платформа як послуга

Модель надання платформи як сервісу (Platform-as-a-Service, PaaS) забезпечує можливість оренди платформи. Платформа як сервіс полегшує розробку, тестування, розгортання і супровід додатків без необхідності інвестицій в інфраструктуру і програмне середовище. Платформа як сервіс також включає і програмне забезпечення як сервіс. Прикладом платформи як сервіс можуть служити Windows Microsoft Azure, Amazon Web Services (AWS), IBM Cloud.

Тут споживачами є самі компанії, які розробили програми. Платформа забезпечує середовище для виконання програм, сервіси по зберіганню даних і ряд додаткових сервісів, наприклад інтеграційні або комунікаційні.

У PaaS постачальник управляє лише апаратною платформою і операційною системою, що обмежує можливості підприємства замовника в управлінні ризиками на цих рівнях.

3. IaaS: інфраструктура як послуга

IaaS (Infrastructure-as-a-Service) – хмарна інфраструктура послуг поставляє комп'ютеру інфраструктуру (наприклад, платформу віртуалізації середовища), сховище і мережу. Замість того, щоб купувати програмне забезпечення, сервера або мережеве обладнання, користувач може купити все це як повністю зовнішній сервіс. Іншими словами, третя сторона за орендну плату дозволяє встановити віртуальний сервер на їх IT-інфраструктури.

У моделі IaaS на стороні замовника можна побудувати свої власні технічні засоби забезпечення безпеки. Клієнт може мати повний контроль над реальною

конфігурацією сервера, що гарантує йому більший контроль ризиків безпеки оточення і даних.

Прикладом компаній. які надають таку послугу є IBM SoftLayer або Amazon Web Services.

Додатково виділяють такі сервіси, як:

- Комунікації як послуга (Communication-as-a-Service, CaaS) – мається на увазі, що в якості сервісів надаються послуги зв'язку; зазвичай це IP-телефонія, пошта та миттєві комунікації (чати).
- Дані як послуга (Data-as-a-Service, DaaS) – надання даних на вимогу користувача незалежно від його географічного розташування або провайдера, або організаційної приналежності.
- Робоче місце як послуга (Workplace-as-a-Service, WaaS) – користувач, маючи в своєму розпорядженні недостатньо потужний комп'ютер, може купити у постачальника обчислювальні ресурси і використовувати свій ПК як термінал, для доступу до послуги.
- Все як послуга (Everything-as-a-Service, EaaS) – комплекс всіляких хмарних сервісів, що задовольняють будь-які IT-потреби.

### 1.3 Переваги та недоліки використання хмарних технологій

На даний момент виділяють чотири моделі розгортання хмарних систем. Вони поділяються на приватні, публічні, громадські та гібридні.

Приватна хмара – це внутрішньокорпоративна хмарна інфраструктура, призначена для обслуговування конкретного підприємства та його філій. Приватна хмара може безпосередньо керуватись замовником або бути доручена зовнішньому підряднику. Від цього залежить розміщення апаратної інфраструктури, яка може бути розташована на території клієнта, так і зовнішнього оператора. Також можливий варіант поділу, коли частина апаратних засобів знаходиться у замовника, а частина у оператора. Ідеальний

варіант приватної хмари – хмара, розгорнута на території організації, що обслуговується та контролюється її співробітниками.

Перевагою моделі приватної хмари перед іншими є можливість здійснення більш детального контролю над ресурсами і розширені можливості їх конфігурації. Крім того, приватні хмари є ідеальним рішенням у разі роботи з конфіденційною інформацією [8]. Але, водночас це може вважатися основним недоліком, оскільки підприємство має можливість самостійно встановити і підтримувати хмарні сервіси. У цьому випадку витрати, пов'язані зі створенням та експлуатацією, лягають на компанію і можуть перевищувати цінність інформації, що обробляється.

Приватним випадком такої інфраструктури можна вважати хмару спільноти (Community cloud), призначену для спільного використання обчислювальної потужності приватної хмари кількома організаціями або особами, які поділяють одні інтереси та вимоги до політики безпеки та керівних документів [9].

Публічна хмара – це хмарна інфраструктура, яка знаходиться у повному розпорядженні постачальника послуг та призначена для вільного використання широкою публікою. Вся відповідальність за встановлення, обслуговування та підтримання працездатності покладається на провайдера. Клієнти, які використовують можливості даного типу інфраструктури, не мають доступу до управління та конфігурування системи та фактично оплачують лише використовувані ресурси у вигляді обчислювальної потужності та абонентського доступу. Абонентом цього типу сервісів може стати як компанія, так і індивідуальний користувач.

Громадська (спільна) хмара – це хмарна інфраструктура, яка призначена для використання конкретною спільнотою споживачів із організацій, що мають спільні цілі (наприклад, місію, вимоги щодо безпеки, політику та відповідність різноманітним вимогам).

Громадська хмара може перебувати у спільній власності, керуванні та експлуатації однієї чи більше організацій зі спільноти або третьої сторони (чи де-

якої їх комбінації). Така хмара може фізично знаходитись як в, так і поза юрисдикцією власника.

Основними перевагами громадських хмар є можливість масштабування проти іншими сервісами і доступність вартості для рядового користувача, з допомогою оплати лише споживаних ресурсів [1].

При цьому головним недоліком даної інфраструктури є найменша можливість конфігурування системи з боку клієнтів, так як дані функції зазвичай є стандартизованими і ґрунтуються на випадках, що найбільше запитуються користувачами випадках. Також не варто забувати про те, що оскільки споживачі не мають можливості управління інфраструктурою, інформація, яка потребує підвищених вимог безпеки та нормативного контролю, не може перебувати в загальнодоступній хмарі через обмежену відповідальність постачальника в цьому питанні.

Гібридна хмара – це інфраструктура, що є поєднанням загальнодоступних і приватних моделей хмар. У цьому типі систем обов'язки з управління розподіляються між провайдером та клієнтом. Даний сервіс надає послуги, що стосуються як приватних, так і публічних хмар [2]. Найбільшу популярність цей тип сервісу має в організацій, мають підвищений рівень активності у певні періоди часу. Завдяки ньому компанії можуть відправляти частину інформації, що не має цінності, на публічну хмару під час складної обробки важливих відомостей, а також надавати через неї доступ користувачам до ресурсів підприємства, що знаходяться в приватній хмарі. Чудово розрахована хмара даного типу дозволяє обробляти інформацію, що має підвищені вимоги до безпеки, так і більш незначну.

Так як подібна концепція є новим рішенням у сфері хмарних обчислень, фундаментальним недоліком гібридних хмар є складність створення оптимального рішення щодо реалізації цієї інфраструктури. Втілення у життя ускладнюються як зміною взаємодії між приватним і загальнодоступним компонентами, і налаштуванням отримання послуг із різних джерел та об'єднанням їх у єдиний блок [4].

Після розгляду переваг та недоліків трьох існуючих моделей розгортання хмарної інфраструктури можна виділити модель приватної хмари, як найбільш безпечну та більшу можливість для конфігурації системи.

## 1.4 Національні та міжнародні стандарти та рекомендації щодо захисту інформації в хмарі

Стандартизація необхідна для ефективного функціонування будь-якої галузі і ринок хмарних послуг не є винятком. Його повноцінний розвиток неможливий без законодавства та стандартів, особливо присвячених захисту інформації, оцінки рівня сервісу, що надається.

Міжнародне товариство проводить активні реформи в законодавчій базі на базі розробки та впровадження стандартів, технічних вимог, правових актів, тим самим сприяючи розвитку новітніх технологій в сфері інформатизації міжнародного суспільства, але на жаль це не стосується України.

В українському законодавстві відсутнє визначення хмарних технологій, проте є суміжні нормативно-правові акти, що стосується їх. Натомість у розпорядженні Кабінету Міністрів Україна від 17 січня 2018 р. «Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації» використовується поняття хмарних технологій, а саме в пункті про напрями цифрового розвитку: «З метою подолання цифрового розриву, створення основ цифрової економіки, реалізації нових можливостей бізнесом та громадянами Кабінет Міністрів України зосереджується на розвитку національних твердих цифрових інфраструктур, зокрема широкосмугової фіксованої телекомунікаційної інфраструктури та мобільної (рухомої) телекомунікаційної інфраструктури, інфраструктури цифрового телебачення, радіо- та технологічної інфраструктури для проектів Інтернету речей, інфраструктури обчислень, віртуалізації та збереження даних (хмарних та туманних), інфраструктури кібербезпеки, спеціалізованих інфраструктур». Та у пункті про гармонізацію з європейськими

та світовими науковими ініціативами зазначається, що «Головним завданням є створення експериментальної бази для проведення досліджень та тестування квантових технологій на розподілених грід- та хмарних інфраструктурах у такій сфері, як програмна інженерія (застосування для Інтернету речей, великих даних, штучного інтелекту)» [10].

Також, в Законі України «Про хмарні послуги» описуються основні аспекти стосовно хмарних провайдерів, обчислень, сервісів та сховищ, що можна прирівняти до використання та згадування хмарних технологій [11].

Для широкого та ефективного впровадження технологій потрібні методичні та нормативні документи, що роз'яснюють, в тому числі, правові рамки застосування цих технологій, наявні проблеми та ризики і способи їх мінімізації. Хмарні технології не є винятком. Однак багато стандартів, які сьогодні застосовуються до хмарних обчислень, були розроблені для «до хмарних» технологій, таких як веб-сервіси та Інтернет. Тому зараз йде активна розробка стандартів і керівництв, призначених для хмарних обчислень.

Традиційно створення нормативно-методичної бази починається з розробки методичних документів на національному рівні. Трохи пізніше з'являються стандарти – національні, а потім і міжнародні.

У багатьох країнах світу розробляються стандарти, в яких викладено рекомендації по використанню хмарних обчислень. Основна увага приділяється питанням забезпечення інформаційної безпеки і захисту персональних даних.

На сьогодні провідними організаціями, що займаються питаннями безпеки в хмарі, є Альянс безпеки в хмарі (Cloud Security Alliance, CSA), що складається з представників IT-індустрії, а також дві державні організації Європи та США: Міжнародна організація зі стандартизації (International Organization for Standardization, ISO) і Національний інститут стандартів і технологій (NIST).

### 1.4.1 Стандарти NIST в сфері хмарних технологій

Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) розробив і опублікував велику кількість стандартів у різних областях для державних, військових та комерційних організацій. Інформаційній безпеці присвячено серію стандартів 800.

NIST взяв на себе лідерство в розробці стандартів хмарних обчислень. Мета – прискорити розгортання в федеральних органах влади США безпечних і ефективних хмарних рішень, які дозволять знизити витрати і одночасно підвищити якість послуг. У NIST була створена спеціальна робоча група по стандартам в сфері хмарних обчислень (Cloud Computing Standards Working Group). Вона провела обстеження існуючого ландшафту стандартів. В якості пріоритетних виділили три області:

- інформаційна безпека;
- інтероперабельность (сумісність);
- вимоги до переносимості хмарних послуг.

Робоча група виявила ряд прогалин в наявних стандартах, починаючи від таких фундаментальних питань, як забезпечення безпеки і захисту особистої інформації, до призначених для користувача інтерфейсів і бізнес-орієнтованих функцій. Також були сформульовані пріоритети в галузі стандартизації для потреб уряду США, зокрема в області аудиту безпеки і відповідності законодавчим актам, управління ідентифікацією та доступом.

NIST сприяє стандартизації систем в області безпеки, сумісності і спрощення зв'язку. Він робить це в рамках своєї програми Jumpstart Adoption of Cloud Computing (SAJACC), яка управляє створенням і впровадженням стандартів хмарних обчислень, пропонуючи демонстраційні приклади, що показують, як можна успішно підтримувати ті чи інші додатки в хмарі.

До основних стандартів, що стосуються хмарних технологій, відносяться:

- NIST SP 800-145 та NIST SP 800-146 [6, 12], які визначають поняття хмарних обчислень та надають загальні рекомендації з їх використання.

- NIST SP 500-292 і NIST SP 500-293 [13, 14], які визначають хмарну архітектуру, основні її компоненти та механізми взаємодії між ними.

- NIST SP 500-292 «Базова архітектура хмарних обчислень» (Cloud Computing Reference Architecture) – це керівництво, що містить модель архітектури та словник, які не залежать від постачальника хмарних послуг. У ньому визначено п'ять ролей (діючих осіб): споживач послуг, постачальник послуг, брокер, аудитор і оператор. Для них і описані словник і базова архітектура. Перехідним на використання хмарних обчислень державним органам рекомендується слідувати викладеним в керівництві визначенням і положенням, щоб забезпечити узгоджене впровадження хмарних послуг.

- NIST SP 800-144 «Керівництво по забезпеченню безпеки і захисту персональних даних при використанні публічних хмарних обчислень» (Guidelines on Security and Privacy in Public Cloud Computing) [7].

Керівництво містить огляд проблем в області безпеки і захисту недоторканності приватного життя, що виникають при використанні публічних хмар, і рекомендації, які слід взяти до уваги організаціям при аутсорсингу даних, додатків та інфраструктури в середовище публічної хмари. В анотації зазначається: «Даний документ дає уявлення про загрози, технологічні ризики і запобіжні заходи, що пов'язані із середовищем публічних хмарних обчислень. Це повинно допомогти організаціям приймати обґрунтовані рішення щодо використання цієї технології ».

- Проект NIST SP 500-299 «Базова архітектура забезпечення безпеки хмарних обчислень» (Cloud Computing Security Reference Architecture) [15].

Документ доповнює керівництво NIST SP 500-292 «Базова (референтна) архітектура хмарних обчислень» повномасштабною моделлю безпеки. Ця модель визначає базовий набір компонентів забезпечення безпеки, рекомендованих для створення успішних і надійних екосистем хмарних обчислень. Документ допомагає зрозуміти взаємозалежність діючих осіб для забезпечення безпеки хмарних сервісів, а також розібратися з вимогами, які повинні сформулювати групи технічного планування і впровадження органів

виконавчої влади, щоб забезпечити придбання хмарних сервісів з рівнями безпеки, що відповідають потребам.

- Стандарт NIST SP 800-125 [16], який описує безпеку технологій повної віртуалізації.

Крім того, загальні стандарти з безпеки, що розроблені NIST, застосовуються до хмарних обчислень, а саме стандарт з керування ризиками, визначення механізмів управління безпекою та конфіденційністю, а також рекомендації з управління безпекою для федеральних інформаційних систем та організацій NIST SP 800-53 [17], безперервний моніторинг безпеки в федеральних інформаційних системах та організаціях NIST SP 800-137 [18], запис до журналу подій безпеки (NIST SP 800-92) та інші.

В липні 2013 року публікацією NIST SP 500-291 [19] було визначено загальні стандарти, що розробляються та прийняті в сфері захисту хмарних обчислень.

### 1.4.2 Стандарти ISO/IEC в сфері хмарних технологій

Основними стандартами, що відносяться до хмарних технологій, належать:

- Стандарт ISO/IEC 17788 «Інформаційні технології – Розподілені прикладні платформи і сервіси - Хмарні обчислення - Загальні положення та словник» (Information technology - Distributed application platforms and services – Cloud computing - Overview and vocabulary) [20].

Стандарт описує концепцію хмарних обчислень і містить ряд термінів і визначень. Він є термінологічної основою для подальшої роботи по стандартизації в сфері хмарних обчислень.

- Стандарт ISO/IEC 17789 «Інформаційні технології - Хмарні обчислення - Еталонна архітектура» (Information technology - Cloud computing – Reference architecture) [21].

Стандарт містить огляд загальних понять і характеристик хмарних обчислень, типів хмар, компонентів хмарних обчислень сторін-учасниць, а також

взаємовідносини між цими елементами. У ньому зроблено наголос на вимоги до того, що повинні забезпечувати хмарні сервіси, а не на питання проектування і впровадження відповідних рішень.

- Технічні специфікації ISO/IEC TS 27017 [22] «Інформаційні технології - Керівництво по заходам інформаційної безпеки для використання сервісів хмарних обчислень, засноване на стандарті ISO/IEC 27002 [23]» (Information technology - Security techniques - Information security management – Guidelines on information security controls for the use of cloud computing services based on ISO/IEC 27002).

Стандарт містить рекомендації щодо забезпечення інформаційної безпеки при хмарних обчислень.

- Стандарт ISO / IEC 27040 «Інформаційні технології - Безпека зберігання даних» (Information technology -Security techniques - Storage security) [24].

Стандарт містить детальні технічні рекомендації щодо того, як організаціям визначити відповідний рівень заходів зниження ризиків шляхом планування, розробки та реалізації системи безпеки при зберіганні даних. У ньому дано огляд загальних уявлень про безпеку при зберіганні даних і відповідні визначення, а також рекомендації, що стосуються типових технологій і сценаріїв зберігання. Стандарт застосовується при забезпеченні безпеки пристроїв і носіїв та відповідних положень управлінської діяльності, а також при забезпеченні безпеки додатків і сервісів. В ньому охоплюються питання безпеки, пов'язані з кінцевими користувачами. Цей стандарт має непряме відношення до хмарних обчислень, так як тема зберігання даних в хмарах порушена в обмеженій мірі.

- Стандарт ISO/IEC 27018 «Звід практик щодо заходів захисту персональних даних при наданні публічних хмарних послуг» (Code of practice for data protection controls for public cloud computing services [25].

Стандарт призначений для постачальників послуг «публічної хмари», які ведуть обробку персональних даних (і, можливо, є операторами персональних

даних). Він містить рекомендації щодо різних аспектів і елементам захисту персональних даних і недоторканності особистої інформації в публічній хмарі.

У ньому будуть визначені додаткові цілі і заходи контролю і управління, пов'язані із захистом персональних даних в хмарному середовищі.

Також цей стандарт розглядається як основа для відповідності вимогам національного та наднаціонального законодавства, містить елементи з європейської Директиви 95/46 ЄС про захист персональних даних, такі, як принципи якості обробки. Він також включає в себе принцип підзвітності.

- Стандарт ISO/IEC 27018: служить доповненням до стандарту ISO/IEC 27001 «Інформаційні технології. Методи забезпечення безпеки. Системи менеджменту інформаційної безпеки. Вимоги» [26], який встановлює загальні вимоги до систем менеджменту інформаційної безпеки.

### 1.4.3 Регламенти GDPR, ENISA, CSA в сфері хмарних технологій

В сучасному цифровому світі, де обмін інформацією стає все більш невід'ємною частиною нашого життя, захист персональних даних стає критично важливим завданням для забезпечення приватності та безпеки громадян. У цьому контексті виникає необхідність уніфікованого і прогресивного правового інструменту, який би регулював обробку особистих даних на теренах Європейського Союзу та Європейського Економічного Простору. Відповідно до цієї потреби 27 квітня 2016 року був прийнятий Загальний регламент про захист персональних даних (GDPR).

EU GDPR (Загальний регламент про захист даних): Цей регламент встановлює правила збору, обробки та зберігання персональних даних громадян Європейського Союзу. Він накладає обов'язки на організації, які опрацьовують такі дані, включаючи хмарних провайдерів.

GDPR є відповіддю на розмаїття викликів, пов'язаних з обробкою персональних даних у цифровому віці. Цей регламент став класичним прикладом правового інструменту, який демонструє прогресивний підхід до захисту

приватності та визначає чіткі норми щодо збору, зберігання, обробки та передачі персональних даних. Він не лише сприяє збереженню довіри громадян до цифрового середовища, але й стимулює інновації та конкурентоспроможність в Європейському Союзі шляхом створення рівних умов для підприємств у сфері обробки персональних даних.

Завдяки введенню GDPR, громадяни мають більшу контроль та здатність регулювати, як їхні особисті дані використовуються, а підприємства зобов'язані дотримуватися високих стандартів захисту особистих даних, що сприяє покращенню кібербезпеки та захисту приватності.

Основними принципами даного регламенту є [27, 28]:

- Легальність, справедливість та прозорість: Обробка персональних даних повинна здійснюватись на законних підставах і з чесними цілями.
- Обмеження мети: Персональні дані можуть збиратись лише для конкретних, визначених і законних цілей, і не можуть оброблятися способом, несумісним із цими цілями.
- Мінімізація даних: Збирання та обробка персональних даних повинні обмежуватись лише тими даними, які є необхідними для досягнення визначених цілей.
- Точність: Забезпечення того, щоб персональні дані були точними і оновлювалися за потреби.
- Обмеження зберігання: Зберігання персональних даних у формі, яка дозволяє ідентифікувати суб'єкта даних, не довше, ніж це необхідно для досягнення цілей, для яких вони були зібрані.
- Цілісність та конфіденційність: Забезпечення безпеки та захисту персональних даних від несанкціонованого доступу, втрати або знищення.

Додатково можна виділити наступні права суб’єктів даних [27, 28]:

- Право на інформацію: Суб'єкти даних мають право на отримання інформації про обробку їхніх персональних даних.

- Право на доступ: Суб'єкти даних мають право отримати підтвердження відповідного контролера щодо обробки їхніх персональних даних та отримати копію таких даних.
- Право на виправлення: Суб'єкти даних мають право на виправлення неточних або неповних персональних даних.
- Право на видалення («Право на забуття»): Суб'єкти даних мають право вимагати видалення своїх персональних даних, коли ці дані більше не потрібні для виконання цілей, для яких вони були зібрані.
- Право на обмеження обробки: Суб'єкти даних мають право обмежити обробку їхніх персональних даних у певних обставинах.

ENISA є агентством Європейського Союзу, створеним з метою забезпечення високого рівня мережевої та інформаційної безпеки в Європі. Засноване в 2004 році, ENISA виконує ряд функцій і завдань, спрямованих на підтримку та координацію ініціатив з кібербезпеки в країнах Європейського Союзу та Європейському Економічному Просторі.

Вона відіграє важливу роль у формуванні стратегій та політик ЄС у сфері кібербезпеки. Шляхом співпраці з країнами-членами та іншими зацікавленими сторонами, агентство сприяє покращенню стійкості та відповідності до вимог з кібербезпеки на всіх рівнях.

Дане агентство опублікувало документи з оглядом хмарних технологій, в яких надається зрозуміла та практична інформація щодо застосування хмарних послуг. У цих документах розглядаються основні поняття та терміни, пов'язані з хмарними технологіями, а також надаються рекомендації щодо забезпечення безпеки в хмарних середовищах. Це такі документи, як «Cloud Computing: Overview & Practical Guidance» та «Cloud Security», що розглядають наступні головні аспекти [29]:

- Архітектура хмарних сервісів: Документ описує різні моделі хмарних сервісів (IaaS, PaaS, SaaS) та їхні особливості з точки зору безпеки.
- Загрози та вразливості: Аналізується спектр загроз та вразливостей, які можуть впливати на безпеку хмарних сервісів.

- Рекомендації з безпеки: Надаються конкретні поради та практичні рекомендації щодо забезпечення безпеки в хмарних середовищах, включаючи аспекти такі як ідентифікація та автентифікація, управління доступом, шифрування тощо.

CSA (Cloud Security Alliance – Альянс безпеки хмар) є некомерційною організацією, що займається збільшенням свідомості та вдосконаленням стандартів безпеки в галузі хмарних технологій. Організація об'єднує фахівців з усього світу з метою розробки і розповсюдження найкращих практик та стандартів безпеки.

Один з ключових документів CSA, що стосується безпеки в хмарних технологіях, – це «Security Guidance for Critical Areas of Focus in Cloud Computing» («Посібник з безпеки для критичних аспектів у сфері хмарних обчислень»). У цьому документі розглядаються різні аспекти безпеки, що стосуються хмарних сервісів, зокрема [31]:

- організаційні та правові питання ІБ;
- технічні питання ІБ.

Крім питань ІБ документ розглядає архітектуру побудови хмари і надає рекомендації та шляхи вирішення цих проблем.

В цілому питання ІБ в хмарі поділяються на дві великі групи: питання управління ІБ в хмарі (організаційні питання ІБ) та ІБ в хмарі під час її використання (технічні питання ІБ). Кожна з груп дробиться на більш дрібні, звані доменами. Домени, що відносяться до організаційних, в першу чергу розглядаються з метою вироблення рішень правових питань, питань політики ІБ, управління ризиками і стандартизації. В рамках технічних питань розглядаються питання реалізації і впровадження захисту в хмарі.

CSA Security, Trust & Assurance Registry (STAR). Ця ініціатива Cloud Security Alliance надає фреймворк для оцінки безпеки хмарних сервісів, а також реєстр провайдерів, які пройшли оцінку відповідно до цього фреймворку.

Дотримання цих стандартів та рекомендацій допомагає забезпечити високий рівень захисту та конфіденційності даних у хмарних сервісах.

## Висновки до розділу 1

Хмарні середовища відіграють важливу роль у сучасному світі інформаційних технологій, надаючи широкий спектр можливостей для зберігання, обробки та розподілу даних та обчислень. З технічної точки зору, хмарні середовища забезпечують масштабовану та еластичну інфраструктуру, яка може відповідати зростаючим потребам користувачів. Бізнес-використання хмарних технологій дозволяє підприємствам ефективно використовувати ресурси, зменшуючи витрати на обладнання та обслуговування інфраструктури.

Однак, важливо пам'ятати про проблеми безпеки та конфіденційності даних у хмарних середовищах. Забезпечення безпеки і захисту приватності залишається важливим завданням для користувачів та провайдерів хмарних послуг. При використанні хмарних середовищ необхідно уважно вивчати умови та політику відповідності, а також вживати заходів забезпечення безпеки, щоб зменшити ризики порушення конфіденційності та цілісності даних.

Усупереч викликам та ризикам, які існують у сфері хмарних технологій, їхні переваги і можливості роблять їх важливим інструментом для сучасних організацій та користувачів. Подальший розвиток і вдосконалення хмарних середовищ буде сприяти зростанню їхнього впливу на глобальний ринок інформаційних технологій.

# РОЗДІЛ 2
# АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ ХМАРНИХ СЕРЕДОВИЩ

## 2.1 Проблеми інформаційної безпеки в хмарних середовищах та прилеглих до них сервісів

При переміщенні даних і додатків в хмари фактично відходять від поняття периметра, на якому будується увесь захист класичних систем – захищатися тепер повинен не периметр та не інфраструктура обробки, зберігання і передачі даних, а сама інформація. Питання безпеки хвилюють не лише клієнта – як провайдер буде звертатися до його даних, але і провайдера – наскільки можна довіряти клієнту, від яких зовнішніх і внутрішніх загроз необхідно забезпечити захист інфраструктури. При цьому основна частка ризиків щодо захисту даних лягає саме на провайдера – постачальника послуг.

Головними проблемами, які виникають в хмарних обчисленнях та потребують подальшого детального аналізу і вирішенні, є такі:

- проблема привілейованих користувачів, що мають привілейований доступ до функцій системи або адміністратори хмарних сервісів. Вони представляють найбільшу загрозу для безпеки інформації в хмарі, а тому для зменшення ризику можливих деструктивних дій з їх боку доцільно вести незалежний нагляд і контроль над їхніми діями в хмарі. Як показує статистика, саме на внутрішніх користувачів припадає найбільша кількість порушень безпеки;
- невідповідність законів в сфері обробки, передачі, зберіганні та захисту інформації різних держав, що є однією з головних проблем, яка гальмує розповсюдження хмарних обчислень. Вирішення цієї проблеми є ключовим фактором для можливості фізичного розміщення серверів постачальника хмарних сервісів в різних країнах і регіонах, а також використання користувачами з різних країн одного постачальника послуг;

- питання довіри до постачальника послуг, які можуть бути вирішені лише за рахунок проведення аудиту безпеки постачальника хмарних послуг і перевірки на відповідність його системи безпеки міжнародним вимогам до захисту інформації, сформульованих в міжнародних стандартах;
- питання загальних вразливостей в хмарі практично нічим не відрізняються від аналогічних в традиційних системах, за винятком того, що знайдена одна вразливість може бути використана для всієї хмари, але в той же час її можна більш легко виправити за допомогою централізованого оновлення, на відміну від традиційних систем. У цей час їх критичність набагато більша, тому що вона може з легкістю вразити всіх користувачів даного постачальника послуг, а тому вимагає превентивних заходів і способів захисту;
- проблеми доступності до сервісів і даних користувачів, відновлення їх роботи після збою або втрати даних повинні вирішуватися на адміністративному і правовому рівнях. При складанні договорів з користувачем повинні бути чітко визначені обов'язки сторін і ступінь їх відповідальності в залежності від обставин подій, які призвели до цих наслідків, а розслідування повинна проводити третя незалежна сторона. Аналогічна проблема існує і в традиційних системах, але користувач має можливість безпосередньо впливати на рівень резервування в системі, яка дає можливість більш гнучко її налаштовувати під конкретні вимоги користувача і його фінансові можливості;
- проблема надання доступу, загального доступу і блокування доступу до ресурсів і даних в хмарі користувачам;
- проблема захисту інтелектуальної власності в хмарі, зокрема програмного забезпечення і даних.

Загалом можна виділити наступні групи проблем інформаційної безпеки, що виникають при використанні хмарних технологій, які гальмують їх широке розповсюдження:

1. Технологічні і організаційні проблеми:

- необхідність зміни класичних (вивчених, відпрацьованих і перевірених) підходів до забезпечення безпеки;

- практично повна відсутність відповідних стандартів по безпеки (особливо в Україні);
- відсутність методик оцінки якості, оцінки ефективності та оцінки захищеності хмарної системи, складність оцінки ризиків;
- недопрацьовані моделі загроз і моделі порушника;
- складності у відстеженні причин порушення безпеки;
- небезпечні програмні інтерфейси (API);
- загроза заволодіння даними провайдером або його співробітниками (інсайдерство) або будь-якої третьої особою;
- відсутність або недостатній контроль над серверами і технологічними процесами;
- специфічні уразливості, що виникають при використанні засобів віртуалізації в хмарах: можливість несанкціонованого взаємодії між хостами і віртуальними машинами, проблеми з ізоляцією хостів і віртуальних машин, різні види атак, що націлені на уразливості гіпервізора;
- специфічні вимоги до ідентифікації і аутентифікації;
- додаткові проблеми захисту підключень вузлів організації до серверів провайдера-постачальника послуг.

2. Юридичні проблеми:

- відсутність стандартів і законодавчих актів;
- розмита область відповідальності через інфраструктуру, що динамічно змінюється.

3. Антропогенні проблеми:

- психологічні складнощі через необхідність передачі даних стороннім компаніям;
- складність оцінки рівня довіри провайдерів;
- недовіра і побоювання нових технологій;
- побоювання скорочень IT-персоналу, що може привести до підвищення ризику інсайдерства.

## 2.2 Класифікація загроз та вразливостей в хмарних середовищах

Класифікація загроз інформаційній безпеці в хмарних середовищах є важливою для розуміння ризиків, з якими можуть стикатися організації, що використовують хмарні послуги. Ось деякі основні категорії загроз [32]:

- Загрози конфіденційності даних.
- Загрози цілісності даних.
- Загрози доступності сервісів.
- Загрози управління ідентифікацією та доступом.
- Загрози управління подіями та аудитом.

До загроз конфіденційності даних належать [32]:

- неавторизований доступ до даних;
- перехоплення даних.

Неавторизований доступ до даних є однією з основних загроз конфіденційності даних в хмарних середовищах. Це відбувається, коли зловмисники отримують доступ до конфіденційної інформації без необхідних дозволів. Такі атаки можуть статися через вразливості в системах аутентифікації, слабкі паролі або використання методів соціальної інженерії [32].

Зловмисники можуть використовувати різні техніки для отримання несанкціонованого доступу, включаючи атаки на паролі, перехоплення сесійних файлів, використання слабко захищених адміністративних інтерфейсів та інші.

У вересні 2017 року американська компанія Equifax, яка спеціалізується на кредитних звітах, стала жертвою однієї з найбільших порушень безпеки даних в історії. Атака призвела до витоку особистої інформації близько 147 мільйонів клієнтів, включаючи імена, адреси, соціальні страхові номери та інші конфіденційні дані. Аналіз показав, що атака сталася через вразливість в програмному забезпеченні, яке не було вчасно виправлено [33].

У серпні 2012 року хмарний сервіс збереження файлів Dropbox став об'єктом атаки, під час якої зловмисники отримали доступ до даних понад 68

мільйонів користувачів. Атака сталася через витік паролів, які були викрадені з інших сайтів та використані для отримання доступу до облікових записів Dropbox [34].

Перехоплення даних відбувається, коли зловмисники отримують доступ до передаваної інформації між користувачем і хмарним сервісом. Це може статися через атаки на мережевий трафік, використання шпигунського програмного забезпечення або атаки Man-in-the-Middle [32].

Атаки перехоплення даних можуть включати перехоплення незашифрованих даних під час їх передачі через небезпечні мережі, використання шпигунського програмного забезпечення на пристроях користувачів або атаки типу Man-in-the-Middle.

У 2016 році компанія Yahoo оголосила про одну з найбільших в історії витоків даних. В результаті атаки було скомпрометовано близько 3 мільярдів облікових записів користувачів. Атака відбулася між 2013 і 2014 роками і включала перехоплення інформації про імена користувачів, електронні адреси, паролі та інші конфіденційні дані [35].

У 2015 році під час атаки на популярний зашифрований месенджер Telegram було виявлено вразливості, які дозволяли зловмисникам перехоплювати та читати зашифровану переписку користувачів. Хоча компанія швидко виправила цю вразливість, але вона привернула увагу до ризиків перехоплення даних в месенджерах.

До загроз цілісності даних належать:

- втрата або зміна даних;
- віруси та інші шкідливі програми.

Втрата або зміна даних може виникати внаслідок технічних проблем, таких як відмова обладнання, помилки в програмному забезпеченні або природні катастрофи. Наприклад, некоректна робота жорстких дисків може призвести до втрати даних, а помилки в програмному забезпеченні можуть призвести до їхньої неправильної зміни або пошкодження [32].

Зловмисники можуть отримати доступ до системи хмарного сховища через недоліки в системі безпеки, слабкі паролі або соціальну інженерію. Після отримання доступу вони можуть змінювати, видаляти або пошкоджувати дані, що зберігаються в хмарному середовищі.

У 2011 році мережа Sony PlayStation була скомпрометована групою зловмисників, які здійснили несанкціонований доступ до бази даних користувачів. В результаті цього було викрадено особисті дані мільйонів користувачів, включаючи їхні імена, адреси та номери кредитних карт. Цей інцидент призвів до серйозного порушення довіри користувачів до компанії Sony [36].

У 2016 році компанія Uber зазнала серйозного порушення безпеки, внаслідок чого було викрадено дані понад 57 мільйонів користувачів та 600 тисяч водіїв. Зловмисники здійснили несанкціонований доступ до бази даних Uber через недоліки в їхній системі безпеки [37].

Шкідливе програмне забезпечення, таке як віруси, черви, троянські програми тощо, може інфікувати хмарні середовища через недостатню безпеку або через використання вразливостей у програмному забезпеченні. Вони можуть поширюватися через електронну пошту, завантаження файлів або вразливості в мережевих протоколах.

У 2020 році компанія SolarWinds, яка постачає програмне забезпечення для моніторингу мереж і систем, стала жертвою супутникового атаки, під час якої зловмисники використовували підроблені оновлення програмного забезпечення для внедрення шпигунського коду у системи клієнтів [38].

Створений у 2010 році, вірус Stuxnet був спрямований на інфільтрацію та руйнування іранських ядерних установок. Він використовував численні вразливості у програмному забезпеченні, щоб переслати себе з комп'ютера на комп'ютер та виконати специфічні команди для пошкодження систем [39].

До загроз доступності даних належать DoS та DDoS атаки.

DoS атака спрямована на перевантаження цільового сервера або мережі запитами, що призводить до тимчасового припинення нормального

функціонування. Це робиться шляхом відправки великої кількості запитів на послуги або ресурси сервера [32, 40].

Зловмисники використовують спеціально розроблені програми або скрипти, щоб надіслати велику кількість запитів на сервер, змушуючи його перевантажитися і стати недоступним для легітимних користувачів. Наприклад, зловмисники можуть використовувати вразливості в мережевих протоколах або програмному забезпеченні для зриву роботи сервера.

DDoS атака є розширеною версією атаки DoS, де зловмисники використовують багато комп'ютерів, які називаються ботнетами, для одночасного відправлення великої кількості запитів на цільовий сервер.

Зловмисники отримують контроль над великою кількістю комп'ютерів, заражаючи їх шкідливим програмним забезпеченням, що дозволяє їм відправляти запити на цільовий сервер. Комп'ютери у ботнеті працюють разом, щоб створити великий об'єм трафіку, який перевантажує цільовий сервер [32, 40].

У 2018 році GitHub став жертвою однієї з найбільших в історії DoS атак. Атака сягнула піку пропускної здатності більше 1,35 терабайт на секунду і викликала проблеми з доступністю сервісу для користувачів по всьому світу [41].

У жовтні 2016 року компанія Dyn, яка забезпечує послуги DNS, стала жертвою складної DDoS атаки. Зловмисники використали ботнет складаючийся з мільйонів заражених пристроїв Інтернету речей (IoT), таких як веб-камери та домашні маршрутизатори, щоб створити неймовірно велику кількість запитів на сервери DNS Dyn. Атака призвела до тимчасової недоступності багатьох популярних веб-сайтів, включаючи Twitter, Netflix та Spotify [42].

У 2007 році хостинговий провайдер EstDomains став жертвою однієї з перших в історії DDoS атак. Атака призвела до тимчасової недоступності деяких сайтів, які були розміщені на серверах EstDomains. Хоча ця атака не була найбільшою в історії, вона відображає перші кроки в еволюції DDoS атак [43].

У червні 2022 року компанія Amazon Web Services (AWS) стала жертвою однієї з найбільших DDoS атак в історії Інтернету. Атака, яка тривала кілька днів,

призвела до тимчасової недоступності деяких послуг AWS для користувачів по всьому світу, включаючи Amazon.com та інші веб-сайти та сервіси, які базуються на AWS [44, 45].

До загроз управління ідентифікацією та доступом належать атаки на ідентифікацію та компрометація облікових записів [32, 40].

Атаки на ідентифікацію – це атаки, які спрямовані на обхід механізмів аутентифікації та отримання несанкціонованого доступу до хмарних ресурсів.

Компрометація облікових записів – це незаконний доступ до облікових записів користувачів або адміністраторів, що може призвести до порушення конфіденційності, цілісності або доступності даних.

До загроз управління подіями та аудитом підлягають наступні:

- маніпулювання журналами подій;
- складність аудиту та виявлення порушень.

Маніпулювання журналами подій (Event Log Manipulation) – це процес зміни чи спотворення записів у системних або програмних журналах подій з метою приховування незаконних або шкідливих дій, або зміни інформації, щоб змінити хід розслідування. Механізмами таких типів загроз є:

- Фальшиві записи: Атакувач може створити фальшиві записи подій, які призводять до збоїв системи чи неправильної інтерпретації подій.
- Видалення записів: Видалення або затирання записів, що містять докази незаконних дій, з журналів подій.
- Зміна часу: Атакувач може змінити час подій у журналах, щоб змінити послідовність подій або зманіпулювати часом виявлення порушення.

Складність аудиту та виявлення порушень (Complexity of Audit and Intrusion Detection) полягає у викликах, пов'язаних з виявленням неправомірної діяльності та виявленням порушень безпеки у великих, складних і динамічних системах.

Причинами даних проблем можуть бути:

- Великий обсяг даних: Загальний обсяг даних у сучасних системах може бути величезним, що ускладнює процес аудиту та аналізу подій.

- Складність мережевої інфраструктури: Сучасні мережеві інфраструктури мають складну топологію та велику кількість вузлів, що робить виявлення порушень складним завданням.
- Висока швидкість змін: У кіберпросторі швидкість змін дуже висока, атаки постійно еволюціонують, що ускладнює виявлення порушень.

Ці загрози представляють лише деякі з потенційних ризиків для інформаційної безпеки в хмарних середовищах. Реальні загрози можуть варіюватися в залежності від специфіки хмарної інфраструктури, типу даних та вимог безпеки конкретної організації.

### 2.3 Класифікація атак спрямованих на хмарні середовища

Розглянемо основні атаки, що спрямовані на хмарні середовища. Посилаючись на різні міжнародні, європейські та національні стандарти можна виділити наступні:

- DoS/DDoS-атаки;
- MitM-атаки;
- атаки з використанням слабкостей програмного забезпечення;
- фішингові атаки;
- SQL-ін’єкції;
- викрадення сеансу (Session Hijacking);
- крос-сайтовий скриптинг (XSS);
- міжсайтова підробка запитів (CSRF);
- переповнення буфера;
- атаки з використанням служб автентифікації та авторизації;
- атаки з використанням вразливостей мережевого протоколу.

DDoS (Distributed Denial of Service) – це тип атаки на комп'ютерну систему або мережу, при якій зловмисники намагаються перевантажити цільовий ресурс або мережу запитами, забираючи доступ до нього легітимним користувачам. У

відміну від звичайних DoS-атак, DDoS використовує розподілену інфраструктуру, що робить виявлення та відхилення атаки складнішим [46].

DDoS-атака зазвичай відбувається за допомогою ботнету, тобто мережі комп'ютерів, що були заражені шкідливим програмним забезпеченням і підконтрольні зловмисникам. Зловмисники відправляють команди до цих комп'ютерів (часто з використанням керуючого сервера), щоб вони одночасно надсилали велику кількість запитів цільовому об'єкту [46]. Приклад реалізації зображено на рисунку 2.1.

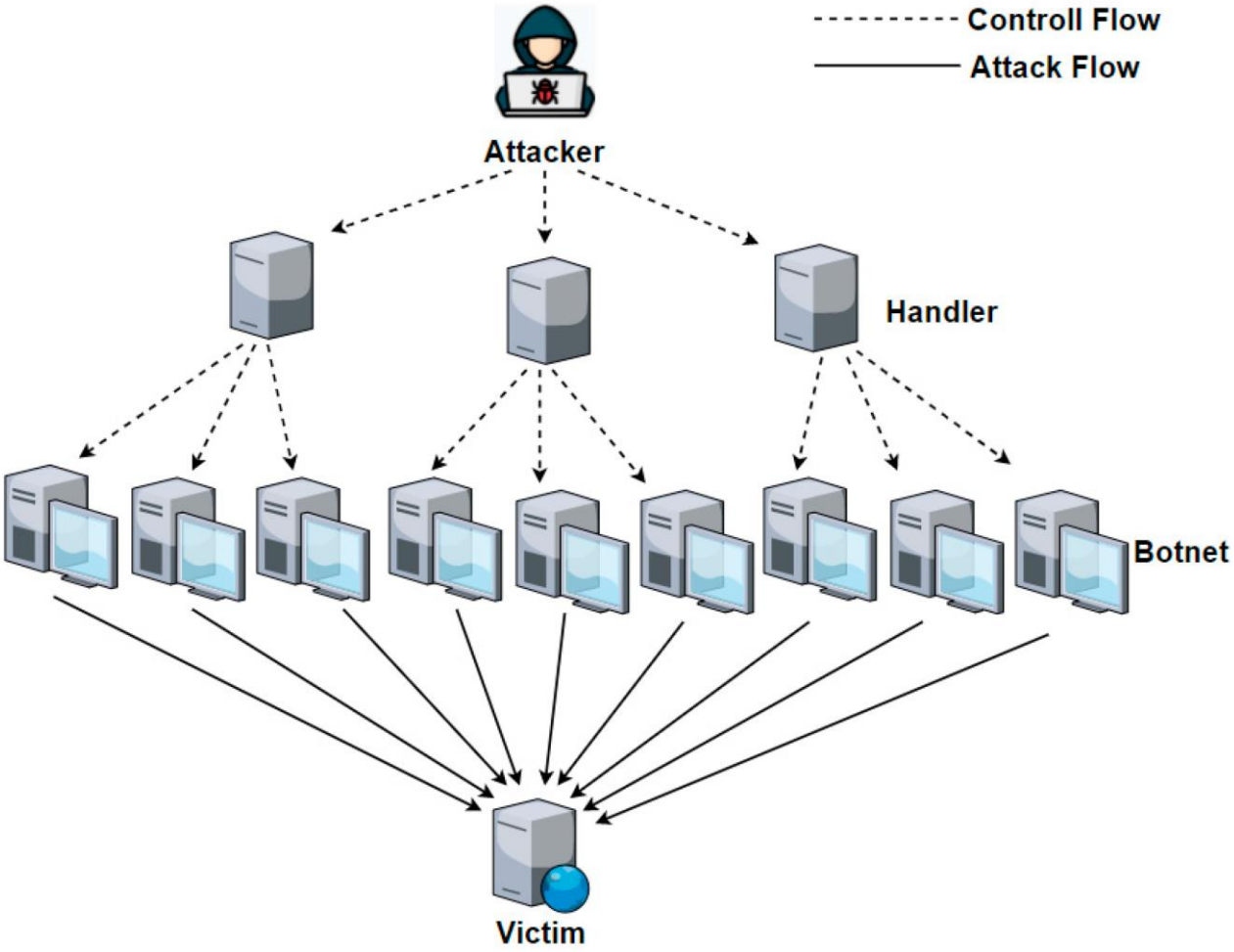


Рисунок 2.1 – Реалізація зловмисниками DDoS-атаки

Основною метою DDoS-атаки є перевантаження мережевих ресурсів цільової системи, таких як мережеві комутатори, роутери або сервери, що призводить до тимчасової відмови в обслуговуванні (DoS) для легітимних

користувачів. Ця атака може спричинити серйозні втрати для організацій у вигляді втрати прибутку, пошкодження репутації та інших негативних наслідків [46].

Серед основних видів DDoS-атак можна виділити атаки на мережевий шар (наприклад, SYN flood), атаки на застосунковий шар (HTTP flood), а також атаки на протоколи, які використовуються для захисту від DDoS (наприклад, DNS або SSL атаки) [46].

Захист від DDoS-атак може включати в себе застосування механізмів фільтрації трафіку на рівні мережі або застосунків, використання розподілених служб захисту, які мають велику пропускну здатність та здатність реагувати на атаки в реальному часі, а також використання CDN (Content Delivery Network) для розподілення навантаження [46].

DDoS-атаки є серйозною загрозою для інтернет-інфраструктури та бізнесу в цілому, і вимагають вдосконалених методів виявлення та захисту для запобігання їх наслідкам.

MitM-атака – це тип атаки, при якій зловмисник вставляється між комунікаційними точками двох сторін і отримує контроль над передачею даних між ними. Зловмисник може перехоплювати, переглядати та навіть змінювати передані дані без відома або згоди сторін [47].

Вона може бути виконана різними способами. Зазвичай зловмисник встановлює контрольований проміжний вузол на маршруті передачі даних, наприклад, захоплюючи бездротовий сигнал Wi-Fi або використовуючи техніки ARP (Address Resolution Protocol) спуфінгу. Після встановлення проміжного вузла, зловмисник може перехоплювати та змінювати передачу даних [47]. Даний вид атаки зображено на рисунку 2.2.

Основною метою цієї атаки є отримання конфіденційної інформації, такої як паролі, особисті дані, банківські дані тощо. Зловмисник може також використовувати цю атаку для впровадження шкідливого програмного забезпечення на систему або для зміни переданих даних з метою введення в оману [47].

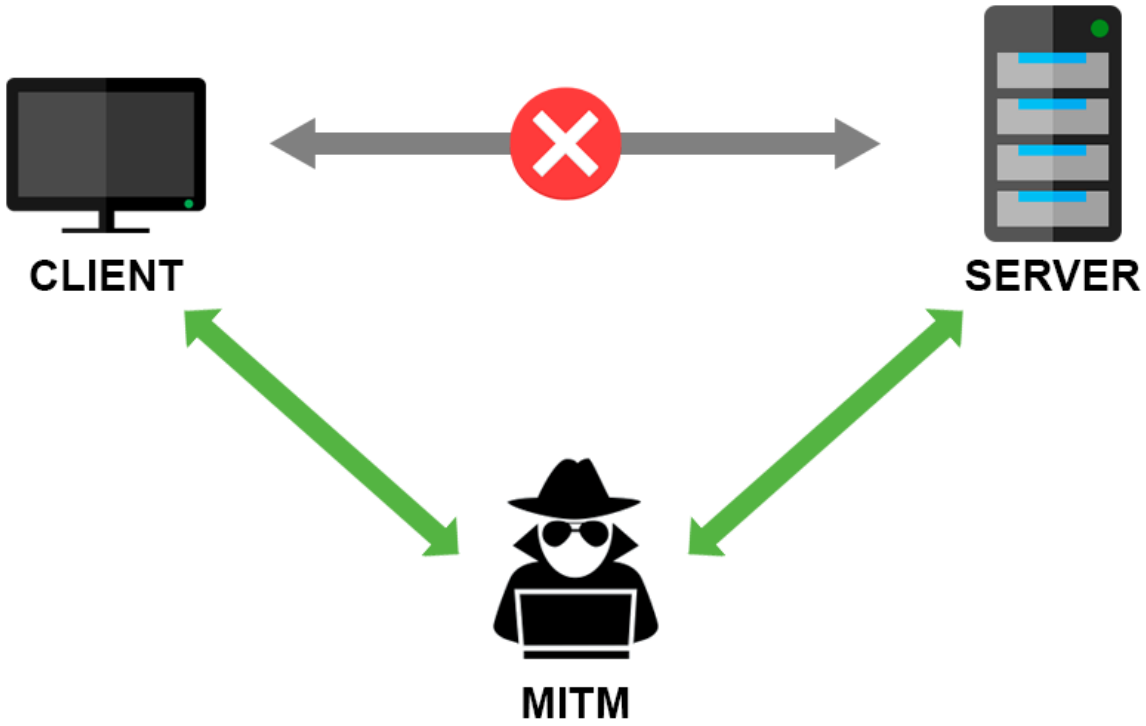


Рисунок 2.2 – Реалізація зловмисником MitM-атаки

Зловмисники можуть використовувати атаки на протоколи шифрування, такі як SSL або TLS, для декодування і перегляду зашифрованих даних [47].

Для захисту від MitM-атак рекомендується використовувати шифрування даних, наприклад, за допомогою протоколів SSL/TLS, використанням VPN (Virtual Private Network), аутентифікацією на основі сертифікатів, а також впровадженням механізмів перевірки цілісності даних, таких як цифрові підписи [47].

Даний вид атаки є серйозною загрозою безпеці, оскільки вони дозволяють зловмисникам отримувати доступ до конфіденційної інформації та втручатися в комунікацію між сторонами без їхнього відома. Захист від таких атак вимагає вдосконалених методів шифрування та перевірки цілісності даних [47].

Атаки з використанням слабкостей програмного забезпечення – це атаки, які використовують вразливості або слабкості в програмному забезпеченні для

незаконного доступу до системи або отримання конфіденційної інформації. Ці вразливості можуть включати недоліки у коді програми, неякісні перевірки введених даних, відсутність або застарілість патчів безпеки тощо [48].

Зловмисники можуть використовувати різні методи для експлуатації вразливостей програмного забезпечення, такі як введення шкідливого коду, виконання SQL-ін'єкцій, використання вразливостей в мережевих протоколах та інші. Ці атаки можуть бути автоматизованими за допомогою інструментів, таких як сканери вразливостей, або виконуватися вручну [48].

Основною метою атак з використанням слабкостей програмного забезпечення є отримання несанкціонованого доступу до системи або сервера, викрадення конфіденційної інформації, виконання шкідливого коду на цільовій системі або створення збоїв у роботі програм [48].

Деякі з найбільш поширених вразливостей включають SQL-ін'єкції, виконання віддаленого коду (Remote Code Execution), вразливості XSS (Cross-Site Scripting) тощо [48].

Для захисту від атак з використанням слабкостей програмного забезпечення важливо регулярно оновлювати програмне забезпечення та встановлювати патчі безпеки, використовувати веб-фаєрволи та інші механізми захисту, а також проводити аудит вихідного коду для виявлення потенційних вразливостей [48].

Атаки з використанням слабкостей програмного забезпечення є однією з найпоширеніших загроз для безпеки інформації в сучасному цифровому світі. Ретельний моніторинг та постійне оновлення програмного забезпечення є важливими заходами для запобігання таким атакам.

Фішингові атаки – це вид атак, в яких зловмисники використовують соціальне інженерство, щоб вивести користувачів з легітимних джерел інформації та змусити їх розкрити конфіденційну інформацію, таку як паролі, особисті дані або банківські реквізити [49].

Фішингові атаки можуть бути виконані через електронну пошту, соціальні мережі, SMS-повідомлення та інші комунікаційні канали. Зловмисники

використовують підроблені повідомлення або веб-сайти, щоб виглядати, ніби вони відомі або надійні джерела, з метою виведення користувачів з легітимних джерел інформації [49].

Основною метою фішингових атак є отримання конфіденційної інформації, такої як паролі, номери кредитних карток або інші особисті дані, які можуть бути використані для шахрайства, крадіжок або ідентифікаційної крадіжки [49]. Наглядний приклад наведено на рисунку 2.3.


Рисунок 2.3 – Фішингова атака зловмисника на жертву з метою отримання важливих даних

Способи фішингових атак можуть варіюватися від масової розсилки електронних листів з пропозиціями про фінансову вигоду до більш цілеспрямованих атак, які використовують персональні дані або контекст спілкування [49].

Для захисту від фішингових атак важливо навчати користувачів розпізнавати підроблені повідомлення, використовувати механізми перевірки двофакторної аутентифікації та ретельно перевіряти URL-адреси перед натисканням на них [49].

Фішингові атаки можуть бути дуже ефективними, оскільки вони використовують людські фактори, такі як довіра та соціальна маніпуляція, для досягнення своєї мети. Захист від таких атак вимагає від користувачів уважності та від організацій - навчання персоналу, впровадження ефективних фільтрів спаму та регулярні аудити безпеки [49].

SQL-ін'єкція – це тип атаки на веб-додатки, яка використовується для введення зловмисного SQL-коду в запити до бази даних (рисунок 2.4). Ця атака дозволяє зловмиснику виконувати небажані SQL-запити або отримувати конфіденційну інформацію з бази даних [50].

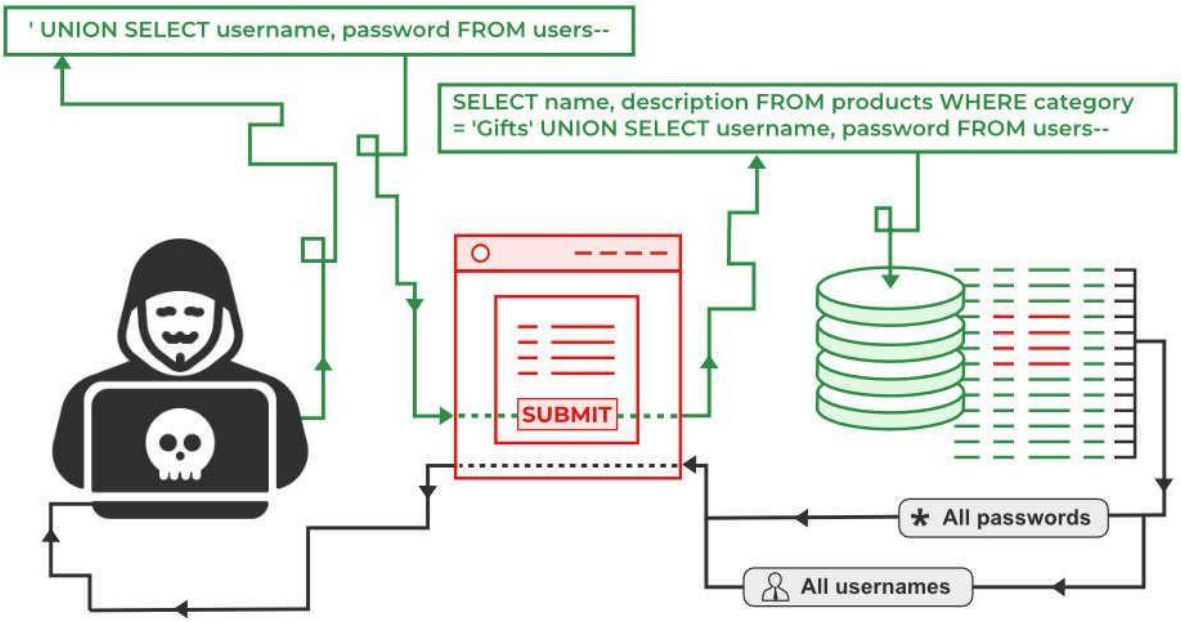


Рисунок 2.4 – Атака зловмисника з використанням SQL-ін’єкцій

SQL-ін'єкції виникають тоді, коли веб-додаток не належним чином обробляє введені користувачем дані перед їх виконанням на сервері баз даних.

Зловмисники можуть використовувати різні методи, такі як введення SQL-коду в форми введення або URL-адреси, для отримання доступу до бази даних [50].

Основною метою SQL-ін'єкцій є отримання несанкціонованого доступу до бази даних, викрадення конфіденційної інформації або виконання небажаних дій на сервері баз даних, таких як видалення або модифікація даних [50].

Деякі типові види SQL-ін'єкцій включають в себе атаки на базові виведення (SQL Injection), вставку (SQL Insertion), оновлення (SQL Update) та видалення (SQL Deletion) даних [50].

Для захисту від SQL-ін'єкцій важливо використовувати параметризовані запити до бази даних, валідацію та екранизацію введених даних, а також використання ORM (Object-Relational Mapping) або інших високорівневих інтерфейсів до бази даних [50].

SQL-ін'єкції є серйозною загрозою для безпеки веб-додатків, оскільки вони дозволяють зловмисникам отримати доступ до конфіденційної інформації та виконувати небажані дії на сервері баз даних. Для захисту від таких атак важливо виконувати належну обробку та валідацію введених даних на всіх рівнях додатка [50].

Викрадення сеансу – це атака, в якій зловмисник намагається заволодіти діючим сеансом аутентифікації між користувачем і системою, зазвичай після того, як користувач успішно автентифікувався.

Ця атака може бути виконана різними способами. Зловмисники можуть перехоплювати та використовувати ідентифікатор сеансу, що передається між користувачем і сервером, або використовувати методи підбору, атаку перехоплення сеансу, а також використання вразливостей в програмному забезпеченні.

Головною метою викрадення сеансу є набуття контролю над сеансом аутентифікації, щоб здійснювати дії в ім'я потерпілого користувача, такі як виконання фінансових операцій, редагування особистої інформації тощо (рисунок 2.5).

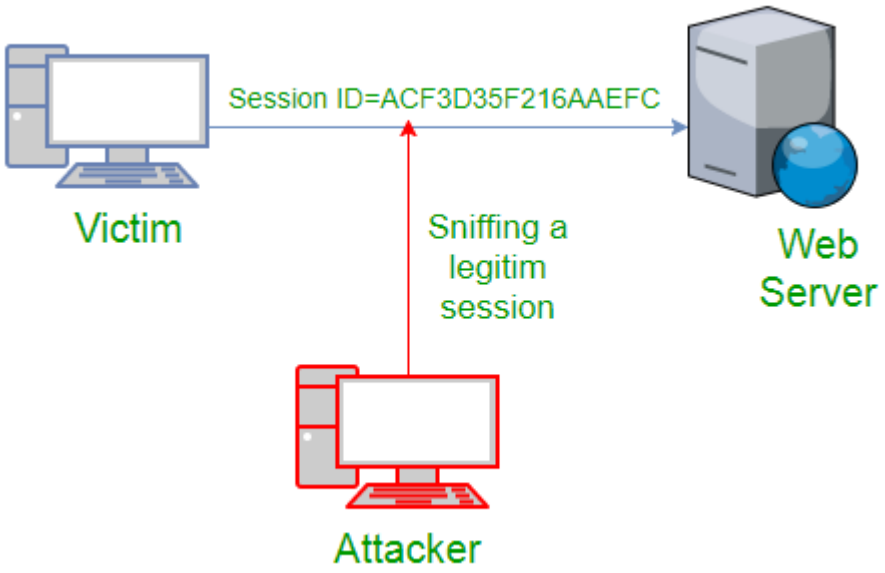


Рисунок 2.5 – Викрадення сеансу автентифікованого користувача

Серед типів атак серед викрадення сеансів можна виділити атаки перехоплення сеансів, атаки фіксації сеансів, а також атаки на багатокористувацькі середовища.

Для захисту від викрадення сеансів важливо використовувати безпечний протокол передачі даних, такий як HTTPS, регулярно оновлювати програмне забезпечення, використовувати механізми перевірки цілісності сеансів, такі як токени аутентифікації, та виявляти та реагувати на підозрілу активність.

Викрадення сеансів є серйозною загрозою для безпеки веб-додатків, оскільки воно дозволяє зловмисникам отримати доступ до сеансів аутентифікації і виконувати дії в ім'я законного користувача. Захист від цієї атаки вимагає впровадження безпечних методів автентифікації та контролю за сеансами, а також моніторингу активності користувачів для виявлення підозрілої поведінки.

Крос-сайтовий скриптінг (XSS) – це тип атаки на веб-додатки, яка дозволяє зловмиснику вставляти та виконувати веб-скрипти на сторінках веб-сайту, які переглядають інші користувачі. Ця атака може призвести до крадіжки сесійних cookie-файлів, перенаправлення користувачів на зловмисні сайти або виконання інших шкідливих дій.

Атака XSS зазвичай використовується через вразливості в веб-додатках, які дозволяють вставляти HTML або JavaScript-код на веб-сторінки без належної обробки. Зловмисники можуть використовувати ці вразливості для введення шкідливого скрипту, який потім виконується у веб-браузері користувача.

Основною метою крос-сайтового скриптінгу є виконання шкідливого коду на сторінках веб-сайту з метою крадіжки конфіденційної інформації, отримання доступу до сесійних cookie-файлів, а також перехоплення та маніпуляція веб-сесіями користувачів (рисунок 2.6).

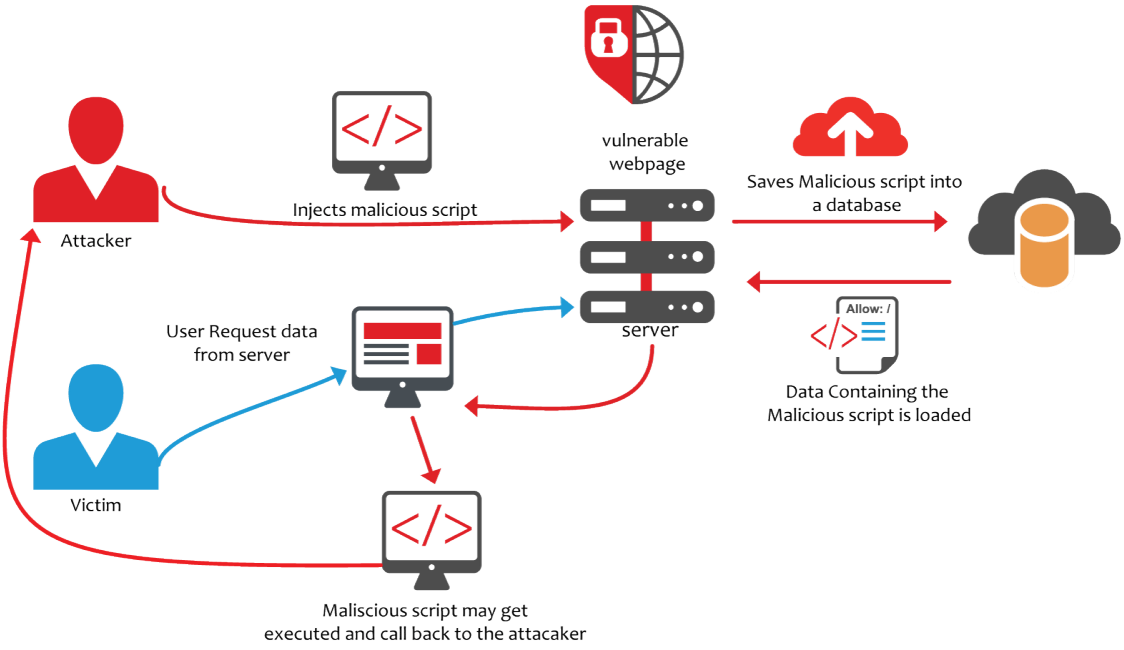


Рисунок 2.6 – Атака зловмисника методом крос-сайтового скриптінгу

XSS може бути здійснений через вразливості у веб-додатках, такі як зберігання даних, відображення та введення даних.

Для захисту від XSS важливо проводити валідацію та екранізацію введених користувачем даних, використовувати HTTP заголовки безпеки, такі як

Content Security Policy (CSP), та регулярно оновлювати веб-додатки для закриття вразливостей.

Крос-сайтовий скриптінг є серйозною загрозою для безпеки веб-додатків і може призвести до серйозних наслідків для користувачів та власників веб-сайтів. Запобігання цій атаки вимагає від розробників веб-додатків використання найкращих практик безпеки програмного забезпечення та регулярної перевірки вразливостей.

Міжсайтова підробка запитів (CSRF) – це атака, при якій зловмисник використовує авторизаційні дані користувача для виконання небажаних дій на веб-сайті, на якому користувач вже авторизований. Ця атака використовує довіру між користувачем і веб-сайтом для здійснення шкідливих дій.

У цій атаці зловмисник створює підготовлені запити, які автоматично відправляються на веб-сайт, де користувач вже авторизований. Ці запити містять команди або інструкції, які змушують веб-сайт виконати небажані дії, такі як зміна паролю, відправлення грошей або видалення даних (рисунок 2.7).

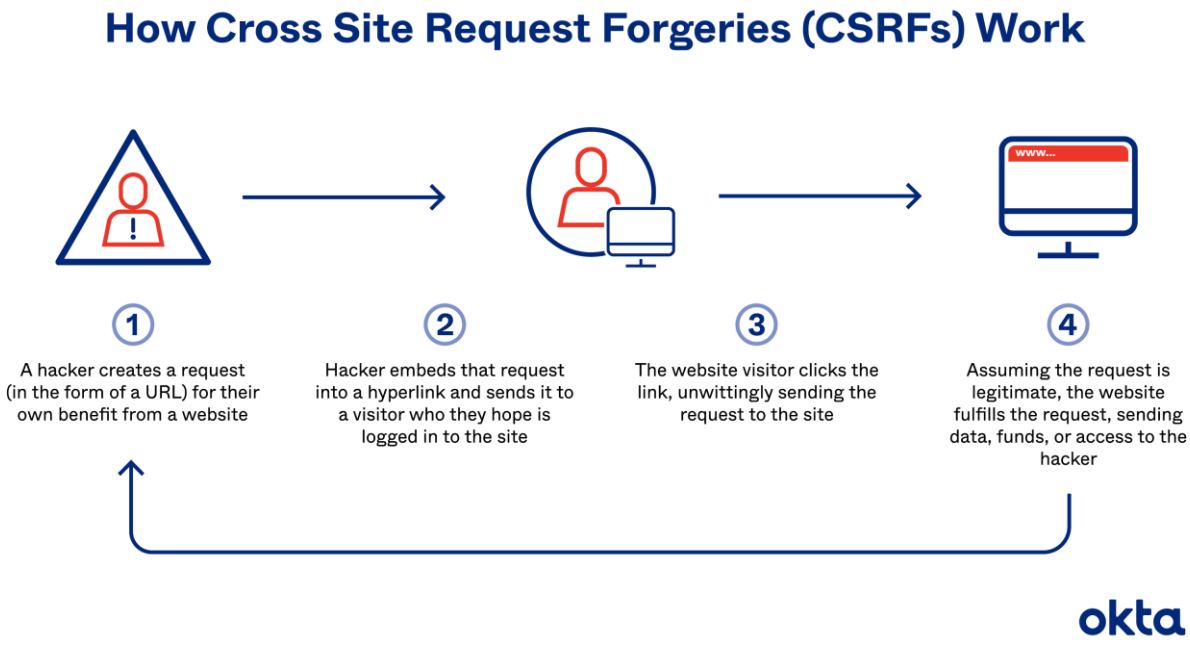


Рисунок 2.7 – Принцип дії міжсайтової підробки запитів

Основною метою CSRF є виконання дій на веб-сайті в ім'я авторизованого користувача без його наочного дозволу. Це може призвести до викрадення чи модифікації конфіденційної інформації, зміни налаштувань або виконання інших шкідливих дій.

CSRF атаки часто використовують сесійні cookie-файли для підтвердження авторизації користувача без його знання.

Для захисту від CSRF важливо використовувати механізми перевірки валідності запитів (наприклад, токени захисту передачі міжсайтових запитів - CSRF токени), використання заголовків HTTP, таких як SameSite cookie, та ретельна перевірка прав доступу при виконанні дій на веб-сайті.

Міжсайтова підробка запитів є серйозною загрозою для безпеки веб-додатків і може призвести до виконання небажаних дій в ім'я авторизованого користувача. Запобігання цій атаці вимагає від розробників веб-додатків використання відповідних захисних механізмів та ретельної перевірки прав доступу.

Переповнення буфера – це вид атаки на програмне забезпечення, при якому зловмисник намагається записати більше даних у буфер пам'яті, ніж він здатний вмістити. Це може призвести до перезапису інших даних в пам'яті, виконання шкідливого коду або збоїв програми.

Під час переповнення буфера зловмисник вводить велику кількість даних у введене поле або вхідні дані, які передаються програмі. Якщо програма не перевіряє розмір буфера перед записом даних, це може призвести до перезапису важливих даних в пам'яті.

Основною метою переповнення буфера є виконання шкідливого коду або отримання несанкціонованого доступу до системи. Зловмисники можуть використовувати цю атаку для запуску власного коду або виклику вразливостей у програмі.

Існує кілька типів переповнення буфера, включаючи стекове переповнення, динамічне переповнення та переповнення купи. Візуальне представлення деяких типів зображено на рисунках 2.8-2.9.

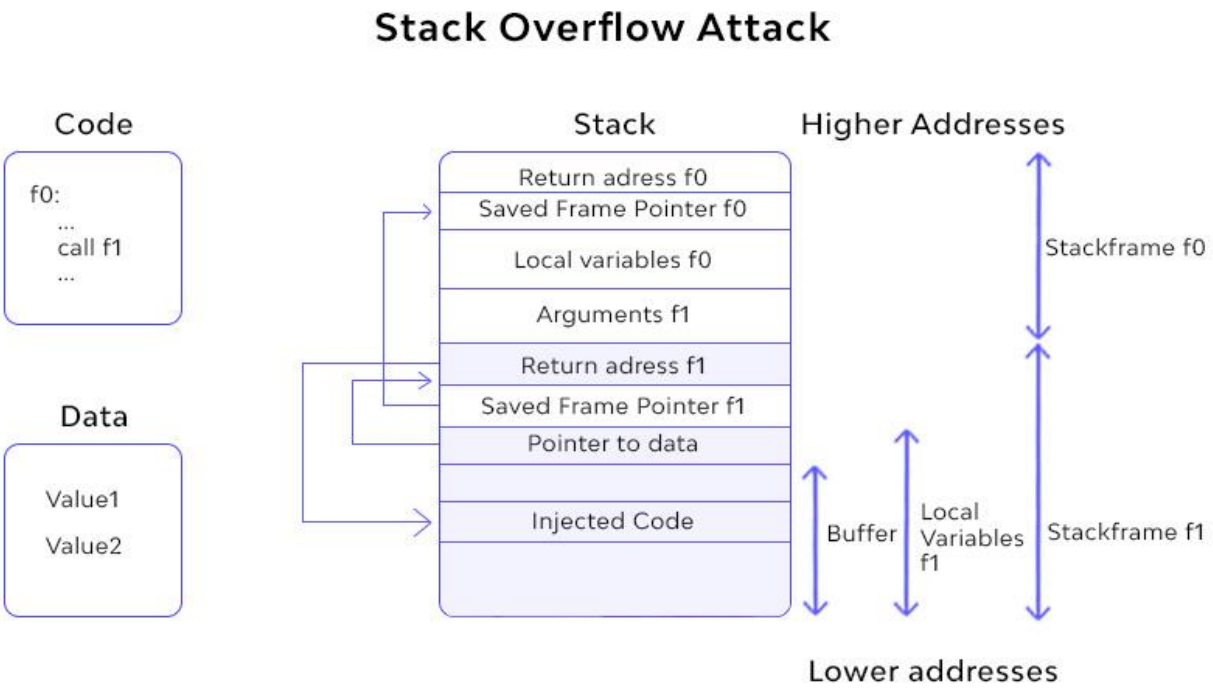


Рисунок 2.8 – Стекове переповнення буфера

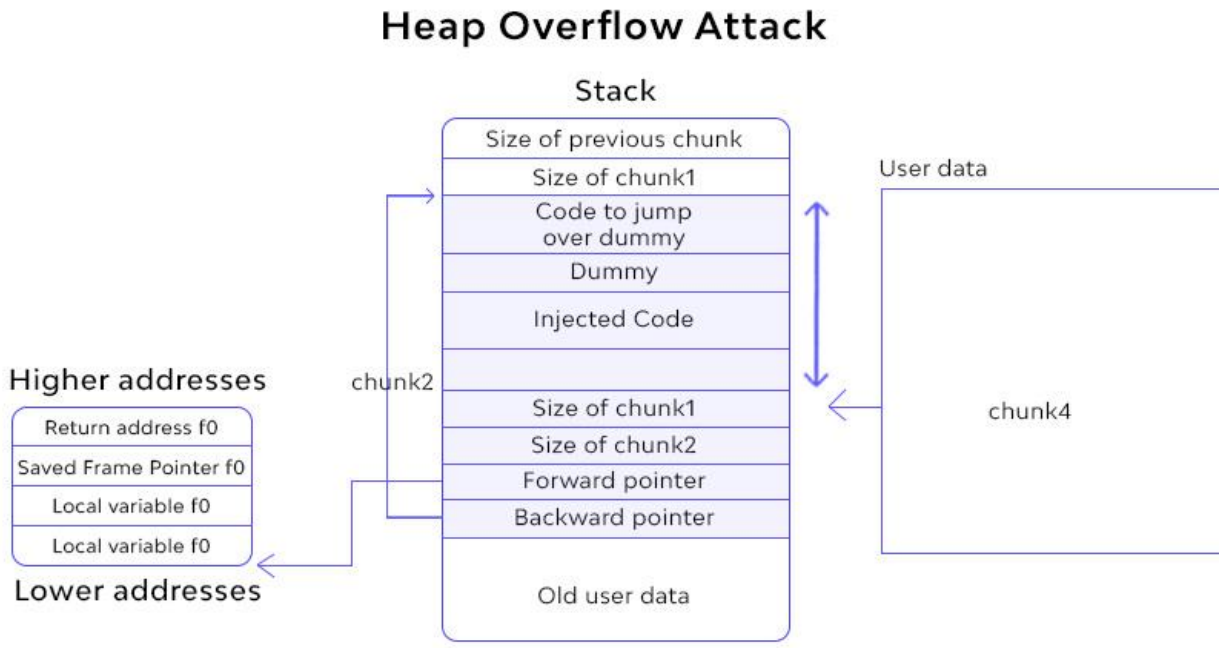


Рисунок 2.9 – Переповнення буфера купи

Для захисту від переповнення буфера важливо використовувати безпечні функції для роботи з буферами, перевіряти вхідні дані на відповідність розміру буфера та використовувати механізми контролю потоку виконання програми.

Переповнення буфера є серйозною загрозою для безпеки програмного забезпечення і може призвести до виконання шкідливого коду або виклику збоїв в програмі. Запобігання цій атаки вимагає від розробників програм використання безпечних методів роботи з буферами та ретельної перевірки вхідних даних.

Атака на служби автентифікації та авторизації – це вид атаки, спрямований на злам системи аутентифікації та авторизації, яка використовується для контролю доступу до ресурсів в інформаційній системі. Ці атаки можуть включати перехоплення аутентифікаційних даних, використання слабких алгоритмів шифрування, обхід авторизаційних механізмів тощо [51].

Ця атака може бути виконана різними способами, включаючи перехоплення паролів, використання методів перехоплення сесій або токенів, форсування паролів, використання слабких механізмів аутентифікації або використання вразливостей у програмному забезпеченні [51].

Головною метою таких атак є отримання несанкціонованого доступу до системи або ресурсів шляхом обходу механізмів аутентифікації та авторизації. Це може дозволити зловмисникам отримати доступ до конфіденційної інформації, виконати несанкціоновані операції або заволодіти контролем над системою [51].

Для підвищення безпеки важливо використовувати двофакторну аутентифікацію для доступу до системи. Важливо моніторити активність користувачів для виявлення підозрілої діяльності та можливих атак [51].

Атаки на служби автентифікації та авторизації є серйозною загрозою для безпеки інформаційних систем і можуть мати серйозні наслідки для організацій та користувачів. Запобігання таким атакам вимагає відповідної конфігурації та моніторингу служб аутентифікації та авторизації, використання найкращих практик безпеки та ретельної перевірки вразливостей програмного забезпечення [51].

Атаки з використанням вразливостей мережевого протоколу можуть включати різноманітні методи зловживання протоколами мережевого зв'язку для здійснення атак на системи та мережеві пристрої [52]. Давайте розглянемо кілька типових атак, які використовують вразливості мережевих протоколів:

ARP Spoofing (ARP підробка). ARP (Address Resolution Protocol) використовується для відображення IP-адрес на MAC-адреси в локальних мережах. ARP Spoofing включає в себе надсилання фальшивих ARP-відповідей для перенаправлення мережевого трафіку на пристрій зловмисника (рисунок 2.10).

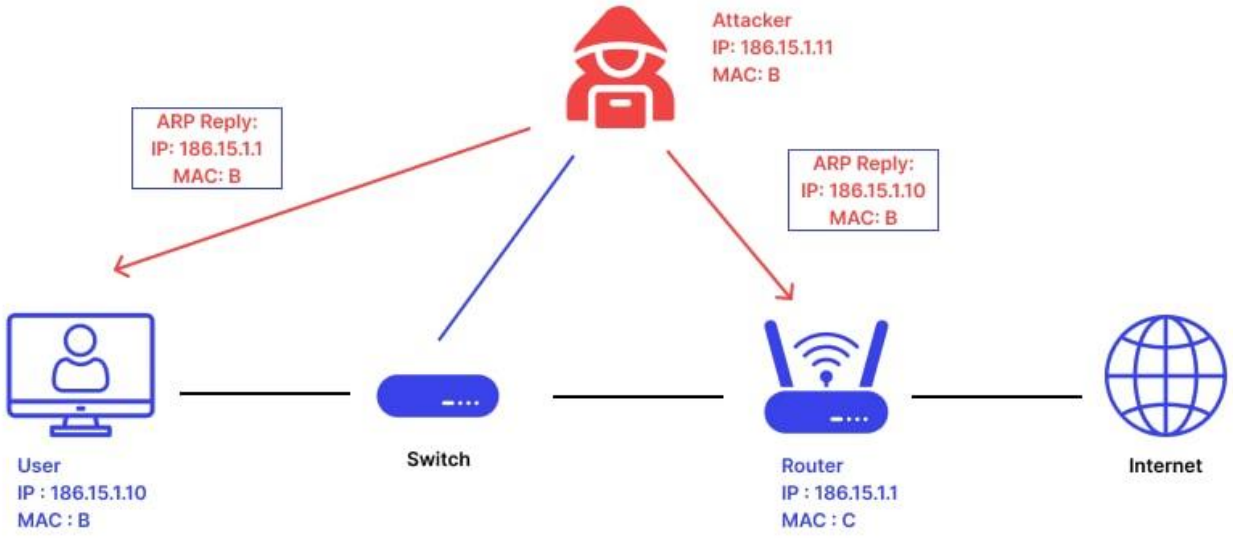


Рисунок 2.10 – Атака на мережу у вигляді ARP спуфінгу

Дана атака здійснюється на мережеві системи задля перехоплення або перенаправлення мережевого трафіку, включаючи чутливі дані.

DNS Spoofing (DNS підробка). DNS (Domain Name System) відповідає за перетворення доменних імен на IP-адреси. DNS Spoofing включає в себе надсилання фальшивих DNS-відповідей для перенаправлення користувачів на підроблені веб-сайти або сервери (рисунок 2.11).

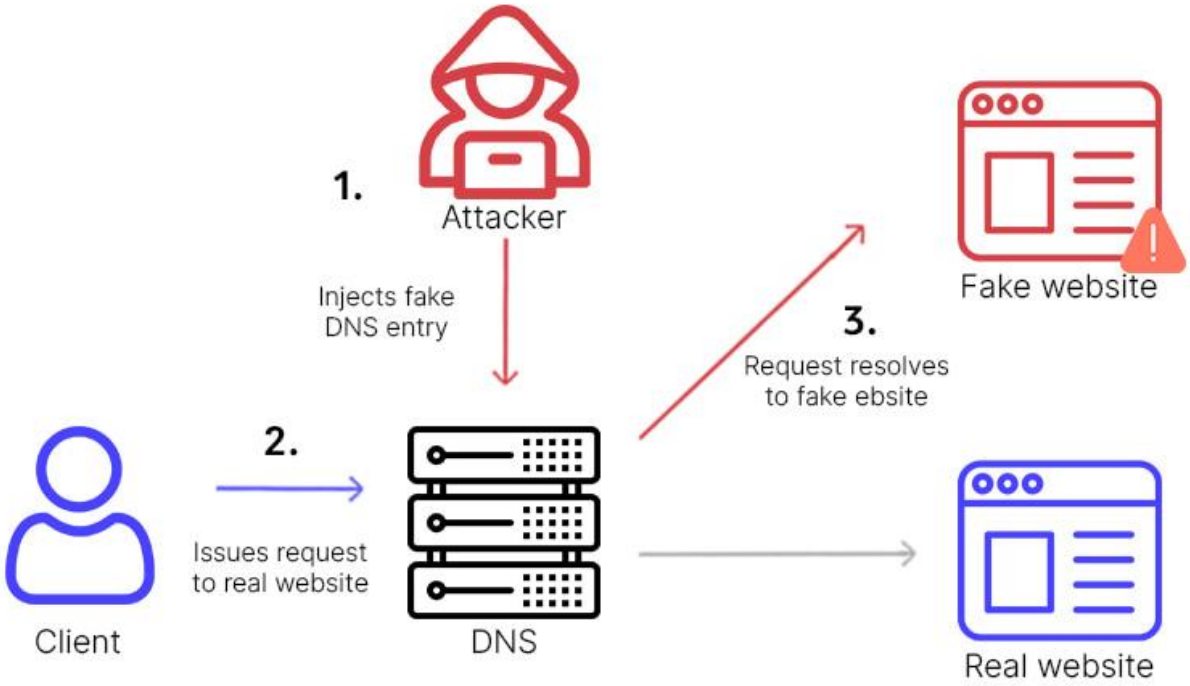


Рисунок 2.11 – Атака на мережу у вигляді DNS спуфінгу

Метою даної атаки є відправлення користувачів на фальшиві веб-сайти з метою крадіжки особистих даних, введення в обман або виконання інших шкідливих дій.

TCP SYN Flooding. Атака використовується для перевантаження сервера шляхом надсилання великої кількості неповних TCP-з'єднань (SYN-пакетів), не завершуючи процесу рукостискання (рисунок 2.12).

Виконання цієї атаки в основному виконується задля недоступності мережевих ресурсів, а саме відмови в обслуговуванні (DoS) або відмови в обслуговуванні на рівні застосунків (DoS-атака на рівні застосунків).

HTTP Session Hijacking. Атака, при якій зловмисник намагається отримати доступ до аутентифікаційних даних сеансу HTTP або сесійних ідентифікаторів для отримання несанкціонованого доступу до облікового запису користувача.

Головною задачею даної атаки є перехоплення сесійних ідентифікаторів або аутентифікаційних даних для несанкціонованого доступу до веб-додатків або облікових записів користувачів.

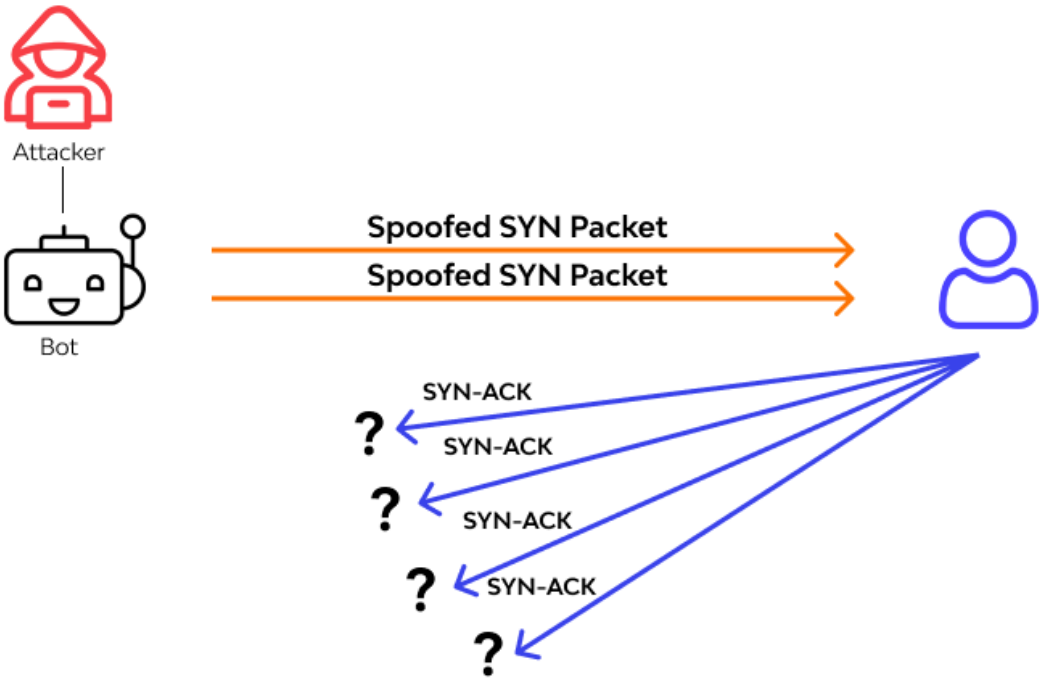


Рисунок 2.12 – Атака на мережу у вигляді TCP SYN Flooding

Ці атаки можуть бути ефективними за умови використання вразливостей мережевих протоколів. Захист від них включає в себе використання шифрування трафіку, встановлення правильних конфігурацій мережевих пристроїв, використання механізмів аутентифікації та авторизації, а також моніторинг мережевої активності для виявлення підозрілих дій.

### 2.4 Заходи захисту та контрзаходи проти атак в хмарних середовищах

Розглянувши в попередньому пункті усі можливі види та типи атак на хмарні середовища, підсумуємо та наведемо заходи захисту та контрзаходи на кожен вид атак з можливим практичним вирішенням їх у вигляді таблиці 2.1.

Таблиця 2.1 – Заходи та контрзаходи протидії атакам на хмарні середовища

| Атака | Вразливість | Загроза | Заходи захисту | Можливе вирішення |
|---|---|---|---|---|
| DDoS-атака | Велика кількість запитів, перевищення мережевих ресурсів | Перевантаження мережі, відмова в обслуговуванні, втрата доступу до сервісу | Використання захисних систем виявлення DDoS, обмеження трафіку, резервне забезпечення мережі, використання мережевих фаєрволів, розподілена охорона, моніторинг мережевого трафіку | Використання CDN, IP-фільтрація, Rate limiting |
| MitM-атака | Некоректна аутентифікація, відсутність шифрування мережевого трафіку | Перехоплення конфіденційних даних, зміна або підробка переданих даних, перенаправлення трафіку | Використання шифрування мережевого трафіку, використання цифрових підписів, перевірка сертифікатів та мультифакторної аутентифікації | Використання SSL/TLS, використання VPN, використання Public Key Infrastructure (PKI) |
| Атаки з використанням слабкостей програмного забезпечення | Неоновлена система, застарілі методи та механізми шифрування | Використання вразливостей для несанкціонованого доступу або витоку інформації | Постійне оновлення програмного забезпечення, використання веб-фаєрволів | Використання веб-застосунків з вбудованим механізмом оновлення |
| Фішинг | Соціальна інженерія, відсутність усвідомлення користувачів | Крадіжка ідентифікаційних та конфіденційних даних | Проведення навчання з безпеки користувачів, регулярне сповіщення про фішингові атаки, фільтрація небезпечних електронних листів, моніторинг активності | Використання електронної пошти зі збільшеними фільтрами спаму та фішингу, маркерів безпеки, подвійна перевірка ідентифікації |
| SQL-ін'єкції | Недостатні перевірки введених даних, вразливості БД | Несанкціонований доступ до бази даних, витік конфіденційної інформації | Використання підготовлених заяв, впровадження заходів захисту в БД | Використання підготовлених заяв з параметризацією, застосування ORM, захисні бібліотеки |
| XSS-атака | Введення небезпечних даних у веб-сторінки | Вибух безпеки, втрата конфіденційності | Екранування введених даних, використання безпечних API, коректна обробка введених даних | Використання Content Security Policy (CSP), санітарні фільтри |

| | | | | |
|---|---|---|---|---|
| Переповнення буферу | Надмірний обсяг даних, що перевищує межі буфера | Вибух безпеки, виконання коду | Використання безпечних функцій, перевірка введених даних, використання механізмів попередження переповнення | Використання захисних функцій, використання механізмів ASLR (Address Space Layout Randomization) |
| CSRF-атака | Використання авторизованих сесійних ідентифікаторів | Виконання небажаних дій в ім'я авторизованого користувача | Використання CSRF-токенів, використання заголовків HTTP, ретельна перевірка прав доступу | Використання SameSite cookie, використання двофакторної аутентифікації |
| Атаки на служби автентифікації та авторизації | Використання вразливих механізмів автентифікації та авторизації, слабкі паролі, атаки перебору паролів | Несанкціонований доступ до системи або ресурсів | Використання безпечних методів автентифікації, використання механізмів моніторингу, регулярне оновлення систем | Використання двофакторної аутентифікації, використання мережевих перегородок (firewalls), аутентифікація біометрією |
| Атаки з використанням вразливостей мережевого протоколу | Використання вразливих протоколів або протокольних реалізацій, недостатні заходи захисту мережі, вразливість мережевих пристроїв | Перехоплення мережевого трафіку, виконання несанкціонованих дій | Шифрування мережевого трафіку, використання аутентифікації на рівні мережі, регулярне оновлення мережевого обладнання, використання мережевих фаєрволів та захищених мережевих протоколів | Використання VPN (Virtual Private Network), використання Intrusion Detection Systems (IDS), мережевий моніторинг та реагування |
| TCP SYN Flooding | Використання TCP SYN-пакетів без завершення рукостискання | Відмова в обслуговуванні мережі | Використання механізмів фільтрації SYN-пакетів, обмеження кількості відкритих з'єднань, використання механізмів мітігації DDoS | Використання SYN cookies, використання SYN/ACK cookies |
| DNS Spoofing | Надання фальшивих DNS-відповідей | Перенаправлення користувачів на фальшиві веб-сайти, перехоплення конфіденційних даних | Використання захищених DNS-систем, перевірка цифрових підписів DNS-відповідей, регулярне оновлення DNS-кешу | Використання DNSSEC, використання DNSSecured DNS резольверів |

| | | | | |
|---|---|---|---|---|
| ARP Spoofing | Відправлення фальшивих ARP-відповідей | Перенаправлення мережевого трафіку, MITM атака | Використання механізмів захисту ARP, моніторинг ARP-таблиць, використання статичних ARP-записів | Використання ARP inspection, використання динамічної ARP-таблиці |
| HTTP Session Hijacking | Недостатня захищеність передачі сесійних ідентифікаторів | Перехоплення сесійних ідентифікаторів | Використання захищеного протоколу передачі даних, використання HTTPS, використання механізмів авторизації зміни сесійних ідентифікаторів | Використання токенів сесії з додатковими заходами безпеки, використання SSL/TLS |

## Висновки до розділу 2

Аналізуючи загрози та вразливості хмарних середовищ, можна визначити, що ці технології не є безпечними від зовнішніх атак та внутрішніх порушень безпеки даних. Найбільш поширеними загрозами є кібератаки, викрадення даних, витік інформації, віруси та шкідливі програми. Крім того, існує ризик порушення конфіденційності, цілісності та доступності даних у хмарних середовищах.

Збільшенням обсягу даних, що зберігаються в хмарних середовищах, зростає ймовірність вразливостей та атак. Тому важливо, щоб провайдери хмарних послуг постійно вдосконалювали свої заходи безпеки, вживали заходів для захисту даних та забезпечення високого рівня конфіденційності.

Все полягає в тому, що хоча хмарні середовища надають багато переваг у зберіганні та обробці даних, вони також мають свої загрози та вразливості. Важливо мати ретельну стратегію безпеки, щоб зменшити ризики порушення безпеки та захисту приватності в хмарних середовищах.

# РОЗДІЛ 3
# ЗАСОБИ ТА МЕХАНІЗМИ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ СЕРЕДОВИЩАХ

У сучасних умовах більшість організацій суттєво автоматизована. Електронний документообіг загалом випереджає традиційний паперовий, а електронна пошта та програми відеоконференцзв'язку на сьогоднішній день вважаються необхідними інструментами для ефективного ділового спілкування [53].

Захист інформації в комп'ютерних системах передбачає систематичне використання засобів і методів, а також прийняття заходів для забезпечення необхідної надійності зберігання та обробки інформації, що здійснюється з використанням комп'ютерної техніки [8].

Відомо, що об'єкт інформатизації, а також система захисту інформації, що створюється для забезпечення його інформаційної безпеки, піддаються впливу загроз інформаційній безпеці. Безпосереднє забезпечення інформаційної безпеки досягається з допомогою використання засобів захисту [54].

Існує три фундаментальні способи забезпечення інформаційної безпеки. Організація інформаційної безпеки може проводитись за допомогою застосування організаційних, апаратних (технічних) або програмних засобів захисту інформації. Найбільша ефективність буде отримана у разі застосування комплексного захисту перерахованих вище способів. Вищезгадані способи можуть бути реалізовані різноманітними засобами.

## 3.1 Організаційні заходи захисту інформації в хмарі

Для захисту периметра інформаційної системи шляхом застосування організаційних засобів створюються:

- системи охоронної та пожежної сигналізації;

- системи цифрового відеоспостереження;
- системи контролю та управління доступом (СКУД).

Захист інформації від витоку технічними каналами зв'язку забезпечується такими засобами та заходами:

- використанням екранованого кабелю та прокладкою проводів та кабелів в екранованих конструкціях;
- установкою на лініях зв'язку високочастотних фільтрів;
- побудовою екранованих приміщень (капсул);
- використанням екранованого обладнання;
- встановленням активних систем зашумлення;
- створенням контрольованих зон тощо.

Також, до важливих організаційних заходів захисту інформації можна віднести наступні пункти:

- проведення аудиту безпеки;
- розробка політик безпеки;
- тренування персоналу;
- класифікація даних;
- управління доступом;
- моніторинг безпеки;
- створення резервних копій;
- оновлення і патчі безпеки;
- засоби шифрування;
- вибір надійного постачальника хмарних послуг.

Перед тим як розпочати використання хмарних сервісів, важливо провести аудит безпеки. Це означає оцінку потенційних ризиків та загроз безпеці, що можуть виникнути в хмарному середовищі.

Створення та впровадження суворих політик безпеки визначатимуть правила та процедури для користувачів, адміністраторів та інших учасників процесу роботи з хмарними даними.

Важливо, щоб персонал був обізнаний з правилами безпеки та процедурами використання хмарних сервісів. Проведення тренінгів і навчання з питань безпеки допоможе зменшити ризик людських помилок.

Також, необхідно класифікувати дані залежно від їхньої чутливості та важливості. Таким чином, це допоможе визначити рівень захисту, який необхідно надати кожному типу даних.

Одним, з найголовніших пунктів, можна визначити вибір постачальника хмарних послуг, який повинен дотримуватися високих стандартів безпеки та має відповідні сертифікати безпеки.

### 3.2 Технічні та програмні засоби захисту хмарних даних

До апаратних засобів захисту належать різні електронні, електронно-механічні, електронно-оптичні пристрої.

До теперішнього часу найбільше поширення отримали наступні апаратні засоби:

- спеціальні регістри для зберігання реквізитів захисту: паролів, кодів, що ідентифікують, грифів або рівнів секретності;
- системи фізичної ідентифікації, такі як біометричні системи, картки доступу та системи розпізнавання обличчя для контролю доступу до дата-центрів та інших об'єктів, де зберігаються сервери хмарних послуг;
- схеми переривання передачі у лінії зв'язку з метою періодичної перевірки адреси видачі даних;
- пристрої для шифрування інформації (криптографічні методи);
- хмарні брандмауери (фаєрволи), які застосовуються для захисту вхідного та вихідного трафіку між хмарними сервісами та зовнішніми мережами;
- спеціалізовані пристрої безпеки мережі.

Програмно-технічні засоби та засоби забезпечення інформаційної безпеки є основою системи захисту інформації. Це сукупність алгоритмів, програм та

протоколів, що забезпечують шифрування, контроль за НСД, захист від шкідливих програм та багато іншого [4].

Існує велика кількість різних додаткових програмних рішень, але розглянемо основні та поширені серед використання.

Системи управління ідентифікацією та доступом (Identity and Access Management, IAM) використовуються для керування ідентифікацією користувачів та контролю доступу до різних ресурсів у хмарному середовищі. Вони дозволяють налаштовувати права доступу для користувачів та груп, встановлювати політики аутентифікації та авторизації, а також відстежувати активність користувачів.

Системи аналізу та виявлення загроз (Threat Detection and Response) використовуються для виявлення та реагування на загрози безпеки у реальному часі. Вони використовують алгоритми машинного навчання та інші методи для аналізу мережевого трафіку, журналів подій та інших даних з метою виявлення несанкціонованих дій та потенційних атак.

SIEM (Security Information and Event Management) – це програмна платформа, яка збирає, аналізує та відстежує інформацію про події та події в системі, що може вказувати на потенційні загрози безпеки. SIEM аналізує дані з різних джерел, включаючи журнали подій, мережевий трафік та дані з безпеки, та використовує алгоритми машинного навчання для виявлення несправностей або аномальної активності, що може свідчити про атаки або порушення безпеки.

DLP (Data Loss (Leak) Prevention) – це програмне забезпечення, яке спрямоване на запобігання втрати конфіденційної інформації шляхом виявлення, моніторингу та контролю активності користувачів та даних у хмарних середовищах. DLP може виявляти та блокувати спроби незаконного виведення даних з системи, моніторити пересилання конфіденційної інформації та застосовувати політики безпеки для її захисту.

IDS (Intrusion Detection System) – це програмне забезпечення, яке виявляє аномальну або підозрілу активність в мережі або системі, що може свідчити про

потенційні атаки або вторгнення. IDS аналізує мережевий трафік та журнали подій для виявлення вразливостей, атак або несправностей у системі.

IPS (Intrusion Prevention System) – це програмне забезпечення, яке доповнює функціональність IDS, додавши можливість автоматичного блокування або відхилення атак або аномальної активності у реальному часі. IPS використовується для негайного реагування на виявлені загрози безпеки шляхом автоматичного блокування та усунення потенційних загроз.

WAF (Web Application Firewall) – це програмний засіб, який використовується для захисту веб-додатків від вразливостей та атак. Він аналізує HTTP-та HTTPS-трафік між веб-додатком та його користувачами і фільтрує або блокує небезпечний трафік, такий як SQL-ін’єкції, Cross-Site Scripting (XSS) або Cross-Site Request Forgery (CSRF).

VPN (Virtual Private Network) – це програмне забезпечення, яке створює зашифроване з'єднання між користувачем та хмарним середовищем через інтернет. Воно допомагає захистити конфіденційні дані під час їх передачі через ненадійні мережі та забезпечує конфіденційність та цілісність даних.

RBAC (Role-Based Access Control) – це програмна модель управління доступом, яка базується на ролях користувачів та дозволяє адміністраторам визначати доступ до різних ресурсів у хмарному середовищі на основі ролей, які вони виконують у організації.

Email Security Gateway – це програмне забезпечення, яке використовується для фільтрації та захисту електронної пошти від шкідливих вмісту, таких як спам, фішингові атаки та віруси. Воно дозволяє виявляти та блокувати небезпечні повідомлення, що допомагає уникнути витоку конфіденційної інформації через електронну пошту.

Container Security Tools – програмні засоби призначені для забезпечення безпеки контейнерів, які використовуються для розгортання та запуску додатків у хмарних середовищах. Вони виявляють та усувають вразливості, контролюють доступ до контейнерів та моніторять їх активність.

Database Security Solutions – програмне забезпечення, яке призначене для захисту баз даних від несанкціонованого доступу, витоку даних та інших загроз безпеки. Воно включає в себе різноманітні інструменти для шифрування даних, моніторингу доступу та виявлення вразливостей баз даних.

Network Traffic Encryption Tools – програмні засоби, які використовуються для шифрування мережевого трафіку між користувачами та хмарними ресурсами, забезпечуючи конфіденційність даних під час їх передачі через мережу.

SOAR (Security Orchestration, Automation, and Response) – це платформи та інструменти, які дозволяють автоматизувати та координувати реагування на інциденти безпеки у хмарних середовищах. Вони поєднують в собі функціональність SIEM, автоматизації та оркестрації для швидкого та ефективного реагування на загрози.

CASB (Cloud Access Security Brokers) – це програмні платформи, які надають широкий спектр функцій для моніторингу, контролю та захисту даних у хмарних середовищах. Вони дозволяють організаціям контролювати доступ до хмарних ресурсів, застосовувати політики безпеки та виявляти небезпечну активність.

CSPM (Cloud Security Posture Management) – це програмні рішення, які використовуються для оцінки та управління безпекою інфраструктури хмарних середовищ. Вони дозволяють ідентифікувати вразливості, налаштувати конфігурації безпеки та виконувати аудит безпеки для забезпечення відповідності з вимогами безпеки.

CWPP (Cloud Workload Protection Platforms) – це програмні рішення, які призначені для захисту робочих навантажень у хмарних середовищах. Вони надають функції моніторингу та захисту віртуальних машин, контейнерів та інших хмарних ресурсів від атак та вразливостей.

SIM (Security Information Management) – це програмне забезпечення, яке використовується для централізованого збирання, аналізу та звітування

інформації про безпеку з різних джерел. Воно дозволяє аналізувати дані безпеки для виявлення та відповіді на загрози.

SWG (Secure Web Gateways) – це програмні рішення, які використовуються для захисту користувачів від шкідливих веб-сайтів та інших загроз у мережі. Вони фільтрують та аналізують веб-трафік для виявлення та блокування небезпечних веб-сайтів та контенту.

### 3.3 Особливості захисту інформації в хмарних середовищах

При побудові мережевої інфраструктури та розміщення в ній хмарі, необхідно враховувати наступні особливості розгортання та побудови захисту.

Хмарні середовища потребують мультирівневого захисту, оскільки вони можуть бути доступні через різні пристрої та мережі. Це означає, що потрібно встановлювати захист на різних рівнях, включаючи мережевий, системний та додатковий захист на рівні додатків.

Однією з особливостей хмарних середовищ є їх здатність до динамічного масштабування, тобто можливість швидко збільшувати або зменшувати обсяг обчислювальних ресурсів в залежності від потреб. З цієї причини системи захисту мають бути гнучкими та здатними адаптуватися до змін у масштабі.

Оскільки дані зберігаються та оброблюються на серверах хмарних постачальників, важливо мати механізми шифрування, які забезпечують конфіденційність інформації від несанкціонованого доступу, а також механізми перевірки цілісності даних, щоб уникнути їх модифікації під час передачі або зберігання.

Також, необхідно враховувати, що хмарні середовища вимагають ефективного управління ключами і ідентифікаторами для забезпечення безпеки. Це включає в себе створення, зберігання та керування ключами шифрування, а також управління доступом до хмарних ресурсів через ідентифікаційні та авторизаційні механізми.

Не менш важливо також забезпечити захист від внутрішніх загроз, таких як несанкціонований доступ співробітників або витік даних через помилки користувачів. Це може включати контроль доступу на рівні користувачів, моніторинг активності та аудит подій.

Важливо мати прозорі механізми безпеки, які дозволяють користувачам перевіряти та переконуватися в тому, що їх дані захищені та що вони дотримуються вимог щодо конфіденційності та безпеки.

При роботі в хмарних середовищах важливо дотримуватися вимог щодо безпеки та відповідності із стандартами, такими як GDPR, HIPAA, PCI DSS тощо. Це може включати проведення аудитів безпеки та забезпечення відповідних заходів захисту даних.

Ще одним з головних факторів є те, що хмарні середовища повинні мати механізми резервного копіювання та відновлення даних для забезпечення стійкості до катастроф, таких як природні лиха або кібератаки, а також для швидкого відновлення після них.

Завдяки дотримання цих особливостей в розгортанні та забезпеченні інформаційної безпеки хмарні середовища будуть працювати надійно на довготривалий час.

**Висновки до розділу 3**

Засоби та механізми захисту інформації в хмарних середовищах відіграють критичну роль у забезпеченні безпеки та захисту конфіденційності, цілісності та доступності даних. Відповідно до найкращих практик у сфері кібербезпеки, провайдери хмарних послуг повинні використовувати комплексний підхід до захисту інформації, який включає в себе різноманітні технічні, організаційні та процедурні заходи.

Технічні заходи включають в себе шифрування даних в спокої та під час передачі, механізми аутентифікації та авторизації, системи виявлення та запобігання вторгнень, резервне копіювання даних та інші технології безпеки.

Організаційні заходи включають в себе розроблення стратегій безпеки, проведення аудитів та перевірок безпеки, навчання та підготовку персоналу щодо захисту даних.

Процедурні заходи включають в себе регулярне оновлення політик безпеки, розроблення інцидентних планів та швидку реакцію на інциденти безпеки.

Загалом, важливо, щоб провайдери хмарних послуг та користувачі взаємодіяли для забезпечення максимального рівня захисту інформації у хмарних середовищах. Це вимагає постійного вдосконалення заходів безпеки та своєчасного реагування на нові загрози та вразливості.

# РОЗДІЛ 4
# ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ХМАРНОМУ СЕРЕДОВИЩІ

## 4.1 Вибір хмарного провайдера з урахуванням вимог безпеки

На сьогодні існує безліч хмарних провайдерів, які користуються великим попитом, зокрема:

- Amazon Web Services (AWS);
- Microsoft Azure;
- Google Cloud Platform (GCP);
- IBM Cloud;
- Oracle Cloud;
- Alibaba Cloud;
- DigitalOcean;
- Rackspace;
- Salesforce;
- VMware Cloud.

Серед даного переліку, виокремимо топ-3 хмарних провайдерів, яким надає перевагу значна кількість людей, компаній та бізнесів. Виходячи з того, що вони користуються даними провайдерами, можна припустити, що в них є важливий перелік сервісів, що відповідає базовим, а також, можливо, поглибленим вимогам інформаційної та кібербезпеки.

Отже, долучимо до топ-3 переліку наступних хмарних провайдерів та розглянемо їх сервіси:

- Amazon Web Services (AWS);
- Microsoft Azure;
- Google Cloud Platform (GCP).

Amazon Web Services (AWS) – це найбільший у світі хмарний провайдер, який надає різноманітні послуги у сфері обчислення, зберігання даних, мереж, інтеграції, аналітики, штучного інтелекту та інших технологій [55].

AWS пропонує широкий спектр послуг, які можна легко масштабувати відповідно до потреб бізнесу. Він має велику мережу дата-центрів по всьому світу, що дозволяє забезпечити високу доступність і надійність сервісів. Однією з його особливостей є те, що постійно впроваджуються нові технології і сервіси, щоб задовольнити потреби зростаючого ринку хмарних обчислень [55].

Переваги AWS:

- користувачі можуть легко масштабувати ресурси в залежності від обсягу роботи;
- пропонується плата лише за використання, що дозволяє бізнесу ефективно використовувати свої фінансові ресурси;
- має регіональні дата-центри по всьому світу, що дозволяє забезпечити низьку затримку і високу доступність.

Недоліки:

- складність для новачків;
- модель ціноутворення «плати за використання» зазвичай ефективна, але великі обсяги ресурсів можуть призвести до значних витрат.

AWS пропонує широкий спектр сервісів. Представимо його в табличному вигляді (табл. 4.1) [56].

Таблиця 4.1 – Перелік сервісів Amazon Web Services

| Категорія | Перелік сервісів |
|---|---|
| Хмарні обчислення | Amazon Elastic Compute Cloud (Amazon EC2), AWS Lambda, Amazon Elastic Container Service (Amazon ECS), Amazon Elastic Kubernetes Service (Amazon EKS), AWS Batch |
| Хмарне зберігання | Amazon Simple Storage Service (Amazon S3), Amazon Elastic File System (Amazon EFS), Amazon Glacier, AWS Storage Gateway |

| | |
|---|---|
| Мережа | Amazon Virtual Private Cloud (Amazon VPC), Amazon Route 53, AWS Direct Connect, AWS Global Accelerator, Amazon CloudFront |
| Бази даних | Amazon Relational Database Service (Amazon RDS), Amazon DynamoDB, Amazon Aurora, Amazon Redshift, Amazon Neptune |
| Аналітика | Amazon Redshift, Amazon EMR (Elastic MapReduce), Amazon Athena, Amazon QuickSight, AWS Glue |
| ШІ та аналіз даних | AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), Amazon Macie, Amazon GuardDuty, AWS Security Hub |
| Розробка та DevOps | AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy, AWS CodePipeline, AWS CloudFormation |

Якщо почати розмову стосовну сервісів забезпечення інформаційної безпеки, то AWS надає широкий спектр для забезпечення безпеки даних та інфраструктури. До них належать [57]:

- AWS Identity and Access Management (IAM);
- AWS Key Management Service (KMS);
- AWS CloudTrail;
- Amazon Inspector.

До найбільш вразливих сервісів AWS, належать:

- Amazon S3;
- Amazon EC2;
- Amazon RDS.

Особливостями Microsoft Azure є його гнучкість, масштабованість, географічна доступність та гармонійне поєднання з іншими продуктами компанії Microsoft такими як Office 365, Dynamics 365 та Windows Server, що спрощує інтеграцію та управління різними сервісами.

Azure пропонує широкий спектр послуг, включаючи обчислення, зберігання, бази даних, мережеві послуги та інші. Користувачі можуть легко масштабувати свої ресурси в залежності від потреб.

Також, має велику кількість дата-центрів по всьому світу, що дозволяє користувачам вибирати регіон для розміщення своїх даних та послуг.

Переваги Microsoft Azure:

- різні сервіси безпеки, такі як Azure Security Center, який надає інтегровану безпеку для ресурсів Azure та розширюється на гібридне середовище.
- пропонує широкий спектр послуг, які можуть задовольнити потреби практично будь-якого бізнесу, від стартапів до великих корпорацій.
- різні моделі ціноутворення, включаючи плату за використання, що дозволяє клієнтам ефективно керувати витратами на хмарні послуги.

Недоліки Microsoft Azure:

- користувачі вважають, що інтерфейс Azure може бути складним для розуміння, особливо для новачків.
- використання більшої кількості послуг може призвести до зростання витрат.

Розглянемо сервіси, які надає даний провайдер. В таблиці 4.2 наведено категорію та перелік сервісів, що надається Microsoft.

Таблиця 4.2 – Перелік сервісів, що надає хмарний провайдер Microsoft

| Категорія | Перелік сервісів |
|---|---|
| Хмарні обчислення | віртуальні машини (Virtual Machines), Azure Kubernetes Service, Azure Functions, Azure Batch, Azure Container Instances |
| Хмарне зберігання | Azure Blob Storage, Azure Files, Azure Disk Storage, Azure Data Lake Storage, Azure Managed Disks |
| Мережа | Azure Virtual Network, Azure Load Balancer, Azure Application Gateway, Azure VPN Gateway, Azure Firewall |
| Бази даних | Azure SQL Database, Azure Cosmos DB, Azure Database for MySQL, Azure Database for PostgreSQL, Azure Cache for Redis |
| Аналітика | Azure Synapse Analytics, Azure HDInsight, Azure Databricks, Azure Data Explorer, Azure Stream Analytics |

| | |
|---|---|
| ШІ та аналіз даних | Azure Machine Learning, Azure Cognitive Services, Azure Bot Services, Azure Data Catalog, Azure Time Series Insights |
| Розробка та DevOps | Azure DevOps, Azure DevTest Labs, Azure Functions, Azure Logic Apps, Azure API Management |

Стосовно сервісів безпеки, то їх лише два, а саме:

- Azure Security Center, що надає централізовану систему моніторингу та управління безпекою ресурсів Azure, забезпечуючи виявлення та відповідь на потенційні загрози.
- Azure Sentinel – є розподіленою системою управління безпекою, яка використовує штучний інтелект для виявлення, аналізу та відповіді на загрози в реальному часі.

Якщо опиратися на існуючі загрози, атаки, та вразливі місця хмарних середовищ та їх сервісів, то в Microsoft Azure можна виділити наступний перелік продуктів:

- Віртуальні машини (Virtual Machines);
- Azure SQL Database;
- Azure Blob Storage;
- Azure Active Directory.

GCP є найменшим по обсягу попиту користувачів серед попередніх двох, але має свою унікальність.

До особливостей, що є й перевагами віднесемо:

- Широкий вибір послуг. GCP пропонує різноманітні послуги, включаючи обчислення, зберігання, бази даних, машинне навчання, штучний інтелект та аналітику даних.
- Швидкість та масштабованість. Інфраструктура GCP побудована на мережі Google, що дозволяє забезпечити високу швидкість мережі та масштабованість.

- Інноваційні технології. GCP постійно впроваджує нові технології та інструменти, що дозволяє користувачам використовувати передові рішення для своїх потреб.

До недоліків даного провайдера можна віднести інтерфейс користувача, так як за відгуками користувачів вказується мала інтуїтивність в порівнянні з іншими хмарними гігантами.

Розглянемо таблицю 4.3 в котрій наведено перелік сервісів, що входять до середовища Google.

Таблиця 4.3 – Перелік сервісів GCP

| Категорія | Перелік засобів |
|---|---|
| Хмарні обчислення | Google Compute Engine, Google Kubernetes Engine, Google App Engine, Google Cloud Functions, Google Cloud Run |
| Хмарне зберігання | Google Cloud Storage, Google Cloud SQL, Google Cloud Bigtable, Google Cloud Firestore, Google Cloud Filestore |
| Мережа | Google Virtual Private Cloud (VPC), Google Cloud Load Balancing, Google Cloud CDN, Google Cloud Interconnect, Google Cloud DNS |
| Бази даних | Google Cloud SQL, Google Cloud Bigtable, Google Cloud Spanner, Google Cloud Firestore, Google Cloud Memorystore |
| Аналітика | Google BigQuery, Google Cloud Dataflow, Google Cloud Dataproc, Google Cloud Datalab, Google Cloud Pub/Sub |
| ШІ та аналіз даних | Google Cloud Machine Learning Engine, Google Cloud Natural Language API, Google Cloud Translation API, Google Cloud Video Intelligence API, Google Cloud Vision API |
| Розробка та DevOps | Google Cloud Build, Google Cloud Source Repositories, Google Cloud |
| Моніторинг | Google Cloud Logging, Google Cloud Monitoring, Google Cloud Trace, Google Cloud Debugger, Google Cloud Profiler |

Сервісів безпеки в Google Cloud Platform трішки більше, аніж у Microsoft Azure. Розглянемо їх.

Google Cloud Identity and Access Management (IAM) відповідає за управління доступом користувачів до ресурсів GCP та забезпечення безпеки ідентифікації та авторизації.

Google Cloud Security Command Center – це централізована система моніторингу та управління безпекою, яка надає детальну інформацію про потенційні загрози безпеки.

Google Cloud Armor виконує захист від DDoS-атак і веб-загроз, а також дозволяє налаштовувати правила безпеки на рівні мережі.

Відповідно до розглянутих в попередніх розділах загроз, вразливостей та атак, то найбільш вразливими сервісами Google Cloud Platform є:

- Google Kubernetes Engine (GKE);
- Google Cloud Storage;
- Google Cloud SQL;
- Google Cloud Functions;
- Google App Engine.

### 4.2 Конфігурування безпеки в хмарних сервісах AWS

Налаштуємо параметри безпеки в деяких сервісах провайдера Amazon. Розпочнемо з сервісу Amazon S3. В конфігураційному файлі опишемо властивості, як вказано на рисунку 4.1.

Даний опис відповідає за створення політики доступу, що обмежує доступ лише для певних користувачів або IP-адрес.

Додатково, для захисту конфіденційності даних під час їх передачі та зберігання можна обрати параметри шифрування, а саме Server-Side Encryption (SSE) або Client-Side Encryption.

Ще однією непоганою практикою буде використання шифрування даних, що потім будуть зберігатися в сховищі.

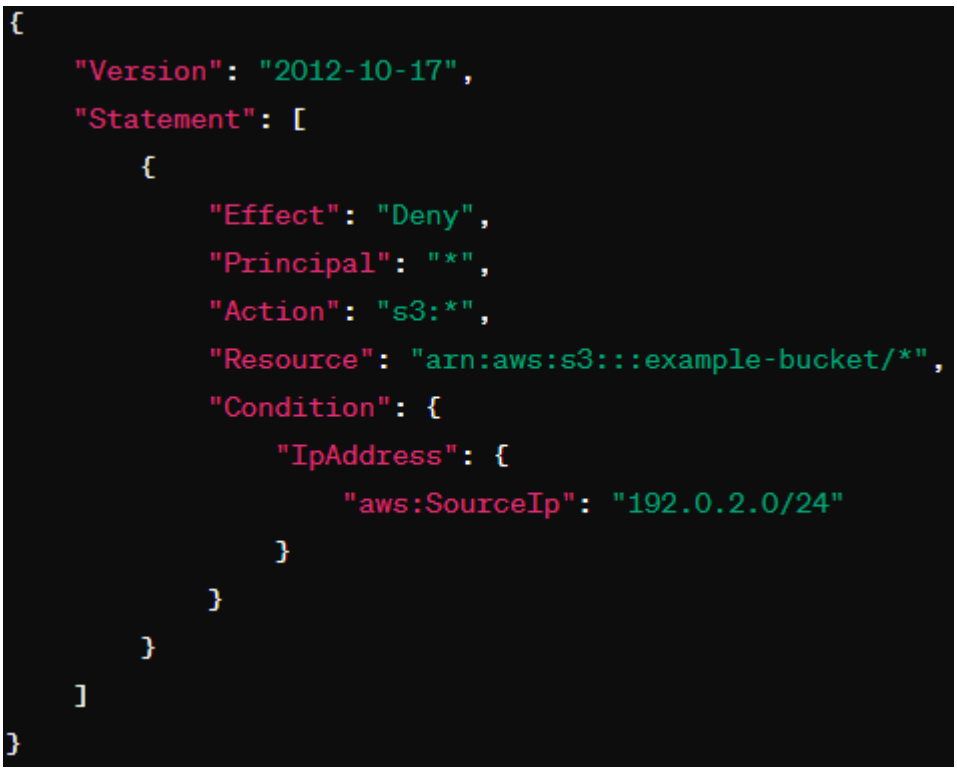


Рисунок 4.1 – Налаштування політики безпеки з обмеження доступу

Розробимо додатково код, що шифруватиме інформацію при передачі до Amazon S3 та розшифровуватиме за допомогою алгоритму AES. Створений код, мовою програмування Python зображений на рисунках 4.2-4.4.

```python
from Crypto.Cipher import AES
import os
import boto3

# Функція для шифрування даних
def encrypt_data(data, key):
    cipher = AES.new(key, AES.MODE_EAX)
    ciphertext, tag = cipher.encrypt_and_digest(data)
    return ciphertext, cipher.nonce, tag
```

Рисунок 4.2 – Опис функції для шифрування даних алгоритмом AES

```python
# Функція для збереження зашифрованих даних у хмарне сховище
def save_to_cloud_storage(data, filename):
    s3 = boto3.client('s3', region_name='your-region')  # Підключення до Amazon S3
    s3.put_object(Bucket='your-bucket', Key=filename, Body=data)

# Функція для завантаження зашифрованих даних з хмарного сховища
def load_from_cloud_storage(filename):
    s3 = boto3.client('s3', region_name='your-region')  # Підключення до Amazon S3
    response = s3.get_object(Bucket='your-bucket', Key=filename)
    data = response['Body'].read()
    return data
```

Рисунок 4.3 – Опис функцій збереження та вивантаження даних

```python
# Основний код
if __name__ == "__main__":
    # Згенеруємо ключ для шифрування
    key = os.urandom(16)  # 16 байтів для AES-128

    # Дані для шифрування
    data = b'Confidential data to be encrypted'

    # Шифруємо дані
    encrypted_data, nonce, tag = encrypt_data(data, key)
  # Зберігаємо зашифровані дані у хмарне сховище
  save_to_cloud_storage(encrypted_data, 'encrypted_data.bin')

  # Завантажуємо зашифровані дані з хмарного сховища
  loaded_encrypted_data = load_from_cloud_storage('encrypted_data.bin')

  # Розшифровуємо дані
  decrypted_data = decrypt_data(loaded_encrypted_data, key, nonce, tag)

  # Виводимо розшифровані дані
  print("Decrypted data:", decrypted_data.decode())
```

Рисунок 4.4 – Головна функція виконання скрипта

Якщо, наприклад, необхідно зробити SecurityGroup для інстансів EC2, яка дозволятиме доступ лише через SSH з визначених IP-адрес, то можна виконати наступні 2 команди:

- aws ec2 create-security-group --group-name MySecurityGroup --description "My security group" --vpc-id vpc-1a2b3c4d
- aws ec2 authorize-security-group-ingress --group-id sg-12345678 --protocol tcp --port 22 --cidr 203.0.113.0/24

У разі необхідності налаштування сповіщень про зміну стану інстансів EC2 можна скористатися конфігурацією AWS CloudWatch створивши правило CloudWatch Events, яке реагує на події зміни стану інстансів EC2 та цільового ресурсу, наприклад Amazon SNS, для сповіщення про ці події (рисунок 4.5).

```
{
  "source": ["aws.ec2"],
  "detail-type": ["EC2 Instance State-change Notification"],
  "detail": {
    "state": ["stopped", "terminated"]
  }
}
```

Рисунок 4.5 – Налаштування сповіщення для інстансів EC2 через AWS CloudWatch

У випадку, коли нам необхідно перемістити файл з одного бакету S3 в інший, то можна скористатися функцією AWS Lambda та подіями Amazon S3. Для цього необхідно:

1. Створити функцію Lambda, яка буде копіювати файли з одного бакету S3 в інший.

2. Налаштувати тригер для створеної функції на події S3 «ObjectCreated» у вихідному бакеті.

3. Використати функцію копіювання об’єктів для переміщення файлів у новий бакет (рисунок 4.6).

```python
import boto3

s3 = boto3.client('s3')

def lambda_handler(event, context):
    source_bucket = event['Records'][0]['s3']['bucket']['name']
    key = event['Records'][0]['s3']['object']['key']
    destination_bucket = "destination-bucket"

    copy_source = {'Bucket': source_bucket, 'Key': key}
    s3.copy_object(CopySource=copy_source, Bucket=destination_bucket, Key=key)
```

Рисунок 4.6 – Функція копіювання об’єктів для переміщення файлів у новий бакет S3

Додатково в це сховище можна налаштувати бекап бази даних RDS. Для цього необхідно створити інстанс RDS, потім створити роль, що буде мати доступ до бакету, а також, призначена до інстансу RDS. Приклад команди наведено на рисунку 4.7.

```
aws rds modify-db-instance --db-instance-identifier your-db-instance \
    --backup-retention-period 7 \
    --preferred-backup-window "00:00-00:30"
```

Рисунок 4.7 – Створення події резервного копіювання бази даних RDS

Додатково, створимо приватну підмережу через VPC та створимо ключ для подальших шифрувань в KMS.

Для налаштування приватної підмережі, виконаємо наступні команди:

- aws ec2 create-vpc --cidr-block 10.0.0.0/16
- aws ec2 create-subnet --vpc-id your-vpc-id --cidr-block 10.0.1.0/24
- aws ec2 create-route-table --vpc-id your-vpc-id

В менеджері ключів:

- aws kms create-key --description "TipaKluch"
- aws kms encrypt --key-id your-key-id --plaintext "VazhliveKrch"

### 4.3 Участь новітніх технологій в хмарному середовищі AWS

AWS пропонує широкий спектр інноваційних сервісів та продуктів, що спираються на потужність ШІ та машинного навчання. Такі рішення допомагають користувачам трансформувати свій бізнес, спрощуючи роботу з хмарними обчисленнями, аналітикою даних, автоматизацією та вирішенням складних завдань. Розглянемо сервіси AWS, які використовують технологію ШІ.

Першим в черзі у нас буде сервіс Amazon SageMaker. Його застосування полягає в тому, що він надає значний набір алгоритмів машинного навчання (градієнтний спуск, випадковий ліс, k-середніх), які можна використовувати безпосередньо без ручного програмування. Враховуючи його застосування для побудови моделей, він дозволяє автоматизовано масштабувати обчислювальні ресурси, щоб навчання відбувалося швидше. Ще однією операцією для покращення та пришвидшення навчання є оптимізація гіперпараметрів моделей. Також, має можливості для розгортання та керування моделями машинного навчання в продукційному середовищі з мінімальними зусиллями.

Наступним цікавим сервісом на базі ШІ є біометричний сервіс Amazon Rekognition. Особливістю є його глибоке вивчення для виявлення та класифікації облич, сцен та об’єктів, що знаходяться на зображеннях та відео. Таким чином, це дозволяє виконувати розпізнавання обличчя у реальному часі задля безпеки чи персоналізації реклами, аналізувати вміст відео та зображень, включно з текстом, що в подальшому дозволяє впроваджувати функції розпізнавання тексту в програмах.

Amazon Comprehend – сервіс обробки природної мови (NLP), яка аналізує текст для виявлення мовних конструкцій, а саме: настрій, сутність, ключові слова та інші мовні аспекти. Він допомагає з аналізом текстів міжнародних компаній, а також, соціальні медіа, веб-сайти тощо.

Amazon Polly – це сервіс синтезу мовлення. Він підтримує кілька стилів голосу та акцентів, що дозволяє використовувати їх в залежності від потреби користувача. Також, непоганим функціональним складом є її використання задля створення аудіо-контенту для сайтів, програм, аудіокниги та автоматизоване читання тексту для користувачів з обмеженими можливостями.

Amazon Lex – це ще один цікавий сервіс, що використовує штучний інтелект. Його задача полягає в комунікації та налаштуваннях взаємозв'язку між різними чат-ботами, незалежно від середовища чи платформи.

Останнім з цього переліку, та доволі корисним сервісом буде Amazon Translate, який використовує нейронну мережу для автоматичного перекладу текстів мовами різних країн та національностей. Він використовується для локалізації веб-сайтів, програмних продуктів, різної документації тощо, що дозволяє користувачам з різних куточків світу отримувати однаково доцільну та повну інформацію.

## 4.4 Рекомендації та засоби щодо уникнення потенційних загроз в критично важливих сервісах AWS

Відповідно до проведених досліджень стосовно вразливостей, загроз та атак, що проводяться на хмарні середовища, а також загальних рекомендацій стосовно їх усунення, створених налаштувань безпеки в сервісах, створимо точні рекомендації із застосуванням сервісів безпеки AWS (таблиця 4.4).

Таблиця 4.4 – Рекомендації та засоби щодо уникнення потенційних загроз в критично важливих сервісах AWS

| Сфера застосування | Рекомендація |
|---|---|
| Аутентифікація та авторизація | • використання міцних паролей або засобів багатофакторної аутентифікації (MFA);<br>• обмеження доступу на основі принципу найменшого привілею (least privilege);<br>• використання AWS IAM для керування доступом до ресурсів. |

| | |
|---|---|
| Захист даних | • використання AWS KMS для керування ключами шифрування;<br>• шифрування даних в спокої (data at rest) та під час передачі (data in transit). |
| Моніторинг та аудит | • використання AWS CloudTrail для запису дій;<br>• використання Amazon CloudWatch для моніторингу метрик та логів системних подій. |
| Захист мережі | • використання Amazon VPC для ізоляції ресурсів;<br>• правильне налаштування фаєрволів для контролю трафіку в VPC;<br>• використання AWS WAF для захисту веб-програм та API. |
| Захист від вразливостей | • використання AWS Inspector для виявлення потенційних вразливостей;<br>• конфігурування сервісів для вчасного оновлення всіх систем та ПЗ;<br>• використання AWS Security Hub для зведеного аналізу безпеки. |
| Захист від DDoS-атак | • використання AWS Shield для захисту від DDoS;<br>• використання Amazon CloudFront та Amazon Route 53 для захисту від DDoS на рівнях мережі та застосунків. |
| Резервне копіювання та відновлення | • регулярне резервне копіювання даних;<br>• налаштування процедури відновлення;<br>• використання AWS Backup для автоматизації процесу створення резервної копії. |
| Оновлення безпеки | • слідкувати за оновленнями безпеки AWS та власними додатками.<br>• автоматизація процесів оновлення та виправлення вразливостей. |

Також важливими аспектами щодо стану безпеки середовища AWS є навчання та перевірка співробітників, які користуються або конфігурують ті, чи інші сервіси.

У випадках, коли використовуються лише деякі хмарні сервіси, будь-якого провайдера, необхідно організувати та правильно спланувати апаратні та програмні засоби захисту ресурсів. Тобто, описати правильну та сувору політику інформаційної безпеки, встановити та налаштувати моніторингові системи тощо, можливе використання власних захисних розробок. Лише так можна забезпечити найкращий захист в критично важливих сервісах.

## Висновки до розділу 4

Практичні аспекти забезпечення інформаційної безпеки в хмарних сервісах є критичними для забезпечення конфіденційності, цілісності та доступності даних користувачів. Застосування ефективних засобів та механізмів захисту є необхідним для мінімізації ризиків кібератак та витоку інформації.

До основних практичних аспектів забезпечення інформаційної безпеки в хмарних сервісах відносяться використання сучасних алгоритмів шифрування, регулярні аудити та перевірки безпеки, механізми автентифікації та авторизації, а також моніторинг даних та виявлення вторгнень.

Важливо також враховувати регулятивні вимоги та стандарти безпеки при використанні хмарних сервісів, забезпечуючи відповідність з GDPR, HIPAA, PCI DSS та іншими вимогами.

Наприкінці важливо підкреслити, що ефективне забезпечення інформаційної безпеки в хмарних сервісах є відповідальністю як провайдерів, так і користувачів. Спільні зусилля та використання передових технологій та практик дозволять забезпечити високий рівень захисту даних у хмарних середовищах.

# ВИСНОВКИ

Завдання дослідження загальної проблеми захисту інформації в хмарних середовищах ставиться на тлі стрімкого розвитку технологій та поширення хмарних обчислень у сучасному цифровому просторі. Відтак, мета дослідження полягає у виявленні ключових аспектів безпеки даних у хмарних середовищах, аналізі відповідних загроз та вразливостей, а також розгляді сучасних засобів та механізмів захисту, спрямованих на забезпечення конфіденційності, цілісності та доступності інформації.

Розглянуто сутність та основні характеристики хмарних середовищ, а також визначено їх переваги та недоліки в порівнянні з традиційними методами зберігання та обробки даних. Додатково наведено національні та міжнародні нормативно-правові акти, що стосується хмарних технологій взагалом.

Розкрито важливі аспекти, пов'язані із безпекою даних у хмарних середовищах. Виявлено різноманітні загрози, що можуть виникнути при використанні хмарних технологій, а також визначено основні вразливості, які можуть бути використані зловмисниками для отримання несанкціонованого доступу до даних. Створено таблицю з превентивними заходами відповідно до мережевих атак, що можуть здійснюватися на них.

Виконано дослідження різноманітних методів та засобів захисту, які можуть бути використані для забезпечення безпеки даних у хмарних середовищах. Розглянуто сучасні технології шифрування, аутентифікації, контролю доступу та моніторингу, що дозволяють підвищити рівень захисту інформації в хмарних середовищах.

Виконано аналіз хмарних провайдерів, виокремивши з них трьох головних на ринку хмарних технологій. Наведено та опрацьовано базові налаштування безпеки в сервісах середовища AWS, що в подальшому дозволять уникати найпоширеніші загрози та атаки.

Розглянуто вплив новітніх технологій та штучного інтелекту на хмарні середовища сьогодення.

Розроблено сучасні рекомендації відповідно до наявних, на сьогодні, ризиків втрати конфіденційності, цілісності та доступності даних.

Наведено ключові аспекти забезпечення інформаційної безпеки в хмарному середовищі, наголошуючи на важливості систематичного й ретельного планування, впровадження та постійного моніторингу заходів безпеки для запобігання можливим загрозам та вразливостям.

Отже, дослідження надає важливий внесок у розуміння проблеми захисту інформації в хмарних середовищах, а його результати можуть бути використані для розробки та вдосконалення стратегій забезпечення безпеки даних у цифровому просторі.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Chang, V., & Ramachandran, M. (2016). Towards achieving data security with the cloud computing adoption framework. IEEE Transactions on Services Computing, 9(1), 138-151.

2. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1-11.

3. Rouse, M. (2017). Cloud Security. [Електронний ресурс]: https://searchcloudsecurity.techtarget.com/definition/cloud-security

4. Al-Roubaiey, A., Al-Jaroodi, J., & Mohamed, N. (2017). A review on security mechanisms in cloud computing. In Proceedings of the 5th International Conference on Future Internet of Things and Cloud (pp. 29-35). ACM.

5. White J.S., Pilbeam A.W. A survey of virtualization technologies with performance testing. [Електронний ресурс]: http://arxiv.org/pdf/1010.3233.pdf

6. The NIST Definition of Cloud Computing: NIST Special Publication 800-145,7 pages (September 2011) – [Електронний ресурс]: http://csrc.nist.gov/ publications/nistpubs/800-145/SP800-145.pdf

7. Jansen W, Grance T. Guidelines on Security and Privacy in Public Cloud Computing. 2011. 80 p. (NIST Special Publication 800-144). [Електронний ресурс]: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

8. Mather, T., Kumaraswamy, S., & Latif, S. (2009). Cloud security and privacy: An enterprise perspective on risks and compliance. O'Reilly Media, Inc.

9. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., ... & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

10. Про схвалення Концепції розвитку цифрової економіки та суспільства України на 2018-2020 роки та затвердження плану заходів щодо її реалізації.

[Електронний ресурс]: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text

11. Про хмарні послуги. [Електронний ресурс]: https://zakon.rada.gov.ua/laws/show/2075-20#Text

12. Cloud Computing Synopsis and Recommendations: NIST Special Publication 800-146, 81 pages (May 2012). – [Електронний ресурс]: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-146.pdf

13. NIST Cloud Computing Reference Architecture: NIST Special Publication 500-292, 35 pages (September 2011). – [Електронний ресурс]: https://bigdatawg.nist.gov/_uploadfiles/M0008_v1_7256814129.pdf

14. US Government Cloud Computing Technology Roadmap: NIST Special Publication 500-293, 140 pages (October 2014). – [Електронний ресурс]: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.500-293.pdf

15. NIST Cloud Computing Security Reference Architecture: NIST Special Publication 500-299, 204 pages. – [Електронний ресурс]: https://bigdatawg.nist.gov/_uploadfiles/M0007_v1_3376532289.pdf

16. Guide to Security for Full Virtualization Technologies: NIST Special Publication 800-125, 35 pages (January 2011). – [Електронний ресурс]: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-125.pdf

17. Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53, 462 pages (April 2013). – [Електронний ресурс]: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf

18. Information Security Continuous Monitoring For Federal Information Systems And Organizations: NIST Special Publication 800-137, 80 pages (September 2011). – [Електронний ресурс]: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf

19. NIST Cloud Computing Standards Roadmap: NIST Special Publication 500-291, 113 pages. – [Електронний ресурс]: https://www.nist.gov/sites/

default/files/documents/itl/cloud/NIST_SP-500-291_Version-2_2013_June18_FINAL.pdf

20. ISO/IEC 17788:2014 Information technology – Cloud computing – Overview and vocabulary. – impl. 15.10.2014. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 16 p.

21. ISO/IEC 17789:2014 Information technology – Cloud computing – Reference architecture. – impl. 10.10.2014. – Brussels: European Committee for Electrotechnical Standardization, 2014. – 53 p.

22. ISO/IEC 27017:2015, Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services (FDIS). – impl. – (October 2014). – Brussels: European Committee for Electrotechnical Standardization, 2014. – 30 p.

23. ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls. – impl. – (October 2013). – Brussels: European Committee for Electrotechnical Standardization, 2013. – 80 p.

24. ISO/IEC 27040:2015, Information technology – Security techniques – Storage security. – impl. – (January 2015). – Brussels: European Committee for Electrotechnical Standardization, 2015. – 111 p.

25. ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. – (August 2013). – Brussels: European Committee for Electrotechnical Standardization, 2013. – 23 p.

26. ISO/IEC 27001:2013, Information technology – Security Techniques – Information security management systems – Requirements. – impl. – (October 2013). – Brussels: European Committee for Electrotechnical Standardization, 2013. – 23 p.

27. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). – [Електронний

ресурс]: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

28. Data protection. Rules for the protection of personal data inside and outside the EU. – [Електронний ресурс]: https://commission.europa.eu/law/law-topic/data-protection_en

29. Cloud Computing Risk Assessment. ENISA. – [Електронний ресурс]: https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

30. Cloud Security. ENISA. – [Електронний ресурс]: https://www.enisa.europa.eu/topics/cloud-and-big-data/cloud-security

31. Security Guidance for Critical Areas of Focus in Cloud Computing, Version 3.0. Technical report, Cloud Security Alliance, 2011. – [Електронний ресурс]: http://www.cloudsecurityalliance.org/guidance/csa guide.v3.0.pdf

32. L. Kenner. CSA's Pandemic 11: Key Cloud Security Dangers & How to Counteract Them. – [Електронний ресурс]: https://www.uptycs.com/blog/the-csas-pandemic-11-top-cloud-security-threats-and-what-to-do-about-them

33. Equifax Data Breach Settlement: What You Should Know. Federal Trade Comission Consumer Advice. – [Електронний ресурс]: https://consumer.ftc.gov/consumer-alerts/2019/07/equifax-data-breach-settlement-what-you-should-know

34. Fergus O'Sullivan. A timeline of Dropbox security issues. – [Електронний ресурс]: https://proton.me/blog/dropbox-security-issues

35. Yahoo Says 1 Billion User Accounts Were Hacked. The New York Times. – [Електронний доступ]: https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

36. Jason Schreier. Sony Estimates Data Breach Costs Of $171 Million. – [Електронний ресурс]: https://www.wired.com/2011/05/sony-psn-hack-losses/

37. Uber Paid Hackers to Delete Stolen Data on 57 Million People. – [Електронний ресурс]: https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data

38. Joe Tidy. SolarWinds: Why the Sunburst hack is so serious. – [Електронний ресурс]: https://www.bbc.com/news/technology-55321643

39. Kim Zetter. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. – [Електронний ресурс]: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

40. ENISA (European Union Agency for Cybersecurity) - Cloud Computing: Benefits, Risks and Recommendations for Information Security. – [Електронний ресурс]: https://www.enisa.europa.eu/media/news-items/cloud-computing-speech

41. Famous DDoS attacks. The largest DDoS attacks of all time. – [Електронний ресурс]: https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/

42. DDoS attack that disrupted internet was largest of its kind in history, experts say. The Guardian. – [Електронний ресурс]: https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

43. Russia accused of unleashing cyberwar to disable Estonia. The Guardian. – [Електронний ресурс]: https://www.theguardian.com/world/2007/may/17/topstories3.russia

44. Michael X. Heiligenstein. Amazon Web Services (AWS) Data Breaches: Full Timeline Through 2023. Firewall Times. – [Електронний ресурс]: https://firewalltimes.com/amazon-web-services-data-breach-timeline/

45. Cloudflare, Google, and Amazon explain what’s behind the largest DDoS attacks ever. The Verge. – [Електронний ресурс]: https://www.theverge.com/2023/10/10/23911186/ddos-http2-vulnerability-blocked-amazon-aws-cloudflare-google-cloud

46. Кирилов, Д. (2021). Understanding DDoS attacks: types, detection and prevention. Digital Defynd. – [Електронний ресурс]: https://www.digitaldefynd.com/ddos-attacks-types-detection-prevention/

47. Man-in-the-middle attack. Microsoft Security. – [Електронний ресурс]: https://www.microsoft.com/security/blog/2022/08/02/man-in-the-middle-attack/

48. Top 10 Web Application Security Risks. OWASP Foundation. – [Електронний ресурс]: https://owasp.org/www-project-top-ten/

49. How to Recognize and Avoid Phishing Scams". Consumer Information. Federal Trade Commission. – [Електронний ресурс]: https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

50. SQL Injection. PortSwigger Web Security. – [Електронний ресурс]: https://portswigger.net/web-security/sql-injection

51. Multi-Factor Authentication. CISA. – [Електронний ресурс]: https://www.cisa.gov/multi-factor-authentication

52. Understanding and Preventing Man-in-the-Middle Attacks. Cisco. – [Електронний ресурс]: https://www.cisco.com/c/en/us/products/security/understanding-preventing-man-in-the-middle-attacks.html

53. Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. Journal of Internet Services and Applications, 4(1), 5.

54. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing (Vol. 800, p. 145). Gaithersburg, MD: National Institute of Standards and Technology.

55. Cloud Computing Services. Amazon. – [Електронний ресурс]: https://aws.amazon.com/

56. Welcome to AWS Documentation. Amazon. – [Електронний ресурс]: https://docs.aws.amazon.com/

57. Cloud Security. Amazon. – [Електронний ресурс]: https://aws.amazon.com/security/