Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Навчально-науковий інститут комп'ютерних наук та штучного інтелекту
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

В.о. зав. кафедрою КІСМіТ
Марина ЄСІНА
"Допущено до захисту"

« »_____2025р.

Пояснювальна записка

до кваліфікаційної роботи бакалавра

на тему: «Методи захисту інформації в хмарних обчисленнях»

оцінка « _____ »

Голова ЕК

Мичуда Л.З.

Керівник: к.т.н. Шеханін К.Ю.

Рецензент: к.т.н. доцент кафедри комп'ютерних систем і мереж ТНТУ Лещинин Ю.З.

Виконавець: студент групи КБ-41
Макаров К.О.

Харків 2025

РЕФЕРАТ

Загальний обсяг основного тексту становить 56 сторінки, включаючи 12 рисунків та 1 таблицю. Перелік використаних джерел налічує 20 найменувань. Робота оформлена згідно з вимогами до кваліфікаційних робіт.

Дипломна робота присвячена аналізу загроз і методів захисту інформації у хмарних обчисленнях. У роботі розглянуто моделі хмарних сервісів, типові вразливості, а також сучасні засоби захисту — зокрема, криптографію, автентифікацію користувачів, контроль доступу та аудит. Особливу увагу приділено практичному дослідженню захисту в сервісах Gmail та Amazon Web Services (AWS).

Робота складається зі вступу, чотирьох розділів, висновків, списку використаних джерел та додатків. У четвертому розділі змодельовано інциденти безпеки: завантаження потенційно шкідливого файлу у Gmail та AWS, аналіз реакції систем на загрозу, а також надано порівняльний аналіз підходів до захисту інформації в обох середовищах.

Актуальність дослідження зумовлена стрімким зростанням популярності хмарних технологій та необхідністю гарантування конфіденційності, цілісності й доступності даних. Запропоновані рекомендації можуть бути використані для підвищення рівня інформаційної безпеки в хмарних сервісах.

Ключові слова: ХМАРНІ ОБЧИСЛЕННЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, КРИПТОГРАФІЯ, GMAIL, AWS, ЗАХИСТ ДАНИХ, ВРАЗЛИВОСТІ, ПРАКТИЧНЕ МОДЕЛЮВАННЯ.

ABSTRACT

The total volume of the main text is 56 pages, including 11 figures and 1 table. The list of references includes 20 sources. The thesis is formatted in accordance with academic requirements.

This thesis is dedicated to the analysis of threats and methods of information protection in cloud computing. The work examines cloud service models, typical vulnerabilities, and modern security measures — in particular, cryptography, user authentication, access control, and auditing. Special attention is given to the practical investigation of security mechanisms in Gmail and Amazon Web Services (AWS).

The thesis consists of an introduction, four chapters, conclusions, a list of references, and appendices. The fourth chapter simulates security incidents: uploading a potentially malicious file to Gmail and AWS, analyzing system responses to the threat, and presenting a comparative analysis of information protection approaches in both environments.

The relevance of the research is driven by the rapid growth of cloud technologies and the need to ensure confidentiality, integrity, and availability of data. The proposed recommendations can be used to enhance the level of information security in cloud services.

Keywords: CLOUD COMPUTING, INFORMATION SECURITY, CRYPTOGRAPHY, GMAIL, AWS, DATA PROTECTION, VULNERABILITIES, PRACTICAL MODELING.

ЗМІСТ

ВСТУП

Сьогодні інформаційні технології розвиваються дуже швидко, і ми щодня користуємось цифровими сервісами — від хмарних сховищ до онлайн-платформ. Це створює потребу у нових способах зберігання й захисту даних. Один із найпоширеніших підходів — це хмарні обчислення. Вони дають змогу працювати з файлами, програмами та сервісами напряму через Інтернет, без потреби у власних серверах.

З активним розвитком хмарних технологій з'являються й нові проблеми у сфері кібербезпеки. Адже коли важливі дані передаються стороннім компаніям, зростає ризик їх втрати або несанкціонованого доступу. Через складність архітектури та систем доступу в хмарі стає важче повністю контролювати безпеку. Тому тема захисту інформації в хмарних обчисленнях є надзвичайно актуальною сьогодні.

Хмарні технології поділяються на кілька моделей надання послуг: інфраструктура як сервіс (IaaS), платформа як сервіс (PaaS) та програмне забезпечення як сервіс (SaaS).

У хмарних обчисленнях існує багато загроз для безпеки даних. Серед основних — перехоплення інформації під час передачі, порушення конфіденційності або цілісності файлів, атаки типу DDoS, помилки або навмисні дії з боку працівників сервісу, слабкий захист акаунтів та уразливості в самому програмному забезпеченні.

Для протидії цим загрозам використовуються різноманітні методи та засоби захисту: криптографічні протоколи, шифрування даних, багатофакторна автентифікація, політики управління доступом, системи виявлення вторгнень, аудит безпеки та інші. Важливим аспектом також є розробка політик безпеки, що враховують специфіку хмарного середовища, а також дотримання міжнародних стандартів і регламентів, таких як ISO/IEC 27001, NIST SP 800-53 тощо.

Мета цієї роботи — розібратися, як саме можна захистити інформацію при використанні хмарних сервісів. Я проаналізував основні загрози та ризики, пов’язані з хмарами, і розглянув, як їм можна протидіяти на практиці. У роботі є приклади типових атак, варіанти захисту, а також описано, як можна побудувати безпечне хмарне середовище на прикладі платформи Gmail.

Актуальність теми обумовлена глобальними тенденціями цифровізації, зростанням обсягів оброблюваної інформації та потребою у надійних механізмах її захисту в умовах використання хмарних технологій. Дослідження у цій сфері сприяють формуванню кращого розуміння загроз, а також впровадженню ефективних рішень у практичній діяльності фахівців з кібербезпеки.

Структура роботи включає вступ, чотири розділи, висновки, список використаних джерел та додатки. Перший розділ присвячено теоретичним основам хмарних обчислень. У другому розглядаються ключові загрози та вразливості, властиві хмарним середовищам. Третій розділ містить аналіз методів та засобів захисту інформації. У четвертому розділі представлено практичну частину – аналіз і моделювання загроз на прикладі платформи Gmail. У завершенні підбиваються підсумки проведеного дослідження та формулюються рекомендації.

У цьому контексті дослідження питань інформаційної безпеки у хмарних обчисленнях є не лише актуальним, а й стратегічно важливим для забезпечення надійної та безпечної цифрової інфраструктури. Вивчення реальних прикладів, моделей загроз, а також впровадження ефективних механізмів захисту сприяє підвищенню загального рівня кібербезпеки як на рівні окремих організацій, так і в державному масштабі.

1 ОСНОВИ ХМАРНИХ ОБЧИСЛЕНЬ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття та принципи роботи хмарних обчислень

Хмарні обчислення (англ. cloud computing) — це спосіб користуватись різними IT-ресурсами (як-от сервери, сховища чи програми) через Інтернет. Користувач може швидко отримувати або відключати ці ресурси без зайвих технічних складнощів. Такий підхід допомагає компаніям зменшити витрати, не будувати власні дата-центри та швидко реагувати на зміни.

Основні характеристики хмарних обчислень, які виділяє Національний інститут стандартів і технологій США (NIST), включають наступне:

Самообслуговування на запит. Користувач сам вирішує, коли і які ресурси йому потрібні, і може отримати їх без звернення до техпідтримки чи адміністратора.

Широкий доступ до мережі. Послуги доступні через Інтернет із використанням стандартних механізмів і клієнтських платформ

Об’єднання ресурсів. Обчислювальні ресурси постачальника об’єднуються для обслуговування багатьох користувачів за допомогою багатокористувацької моделі

Швидка еластичність. Ресурси можуть бути швидко масштабовані (збільшені або зменшені) відповідно до потреб користувача.

Вимірюване обслуговування. Використання ресурсів контролюється, вимірюється та звітується, що забезпечує прозорість для користувачів та постачальників.

Хмарні технології працюють завдяки віртуалізації — це коли замість реального «заліза» створюються віртуальні версії серверів, сховищ чи мереж. Такий підхід допомагає економити ресурси, не купувати зайве обладнання і швидко запускати потрібні сервіси.

Існує кілька типів розгортання хмарних обчислень

Публічна хмара. Інфраструктура надається третім особам через Інтернет. Прикладами є Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform.

Приватна хмара. Інфраструктура використовується виключно однією організацією. Може бути розташована локально або в дата-центрі постачальника послуг.

Гібридна хмара. Комбінація приватної та публічної хмари з метою гнучкого управління навантаженнями.

Мультихмара. Стратегія використання кількох хмарних платформ одночасно, що дозволяє уникнути залежності від одного постачальника.

Розгортання хмарної інфраструктури також передбачає використання таких сервісних моделей:

Інфраструктура як сервіс (IaaS). Користувач отримує доступ до віртуалізованих обчислювальних ресурсів (серверів, сховищ, мережевих компонентів). Він самостійно керує операційними системами, додатками, зберіганням.

Платформа як сервіс (PaaS). Постачальник надає середовище для розробки, тестування і розгортання додатків. Користувач керує лише додатками.

Програмне забезпечення як сервіс (SaaS). Користувач отримує готове програмне забезпечення через Інтернет. Приклади: Gmail, Google Docs, Microsoft Office 365.

Хмарні обчислення мають багато плюсів: їх легко масштабувати, вони гнучкі, дозволяють економити гроші й працювати з будь-якого місця, де є Інтернет. Рішення можна запускати швидко, а оновлення та підтримка часто відбуваються автоматично. Але є й мінуси — наприклад, залежність від стабільного з’єднання, ризики для конфіденційності даних, складність при інтеграції зі старими системами та дотримання різних правил і стандартів.

Перші ідеї, пов’язані з хмарними обчисленнями, з’явилися ще в 1960-х роках. Але реально ця технологія почала розвиватись у 2000-х, коли з’явились великі дата-центри, швидкий Інтернет і потреба у гнучких IT-рішеннях. Зараз хмарні сервіси стали звичними для всіх — ними користуються компанії, державні органи, університети й навіть невеликий бізнес.

Отже, хмарні обчислення — це не просто модна технологія, а основа сучасних IT-систем. Вони змінюють підхід до зберігання, обробки та захисту даних у цифрову епоху.

Одним із важливих принципів хмарних обчислень є «безперервна доступність» (high availability). Це означає, що сервіси повинні працювати без зупинок навіть у разі технічних збоїв. Для цього використовують резервні копії, дублювання даних і автоматичне перемикання на інші сервери.

Ще одна важлива перевага хмарних обчислень — це економія на масштабі. Провайдери обслуговують багато клієнтів одночасно, тому можуть зменшувати вартість послуг завдяки автоматизації та спільному використанню ресурсів.

Також слід зазначити, що сучасні хмарні рішення підтримують концепцію «інфраструктури як коду» (Infrastructure as Code, IaC). Це означає, що адміністратори можуть керувати інфраструктурою за допомогою програмного коду, використовуючи такі інструменти, як Terraform або Ansible. Це значно підвищує швидкість розгортання сервісів, спрощує масштабування та забезпечує відтворюваність середовища.

У сфері хмарних обчислень дуже важливим є питання відповідності чинним законам і стандартам щодо захисту даних. Наприклад, у Європейському Союзі діє регламент GDPR, який захищає персональні дані громадян, а в США у сфері медицини застосовується HIPAA. Крім того, кожна країна може мати свої власні вимоги до зберігання й обробки чутливої інформації. Тому компанії, які користуються хмарними сервісами, повинні переконатися, що обраний провайдер

дотримується всіх необхідних норм. Це стосується і того, як саме обробляються дані, де вони зберігаються, і хто має до них доступ. Якщо провайдер не відповідає таким вимогам — це може спричинити не лише втрату даних, а й юридичні проблеми для самої компанії.

Загалом хмарні обчислення змінюють підхід до побудови IT-інфраструктури. Завдяки їм компанії можуть зосередитись на своїй основній діяльності, не витрачаючи час і ресурси на налаштування серверів чи оновлення систем. Всю технічну частину беруть на себе хмарні провайдери. У результаті бізнес працює ефективніше, швидше впроваджує нові рішення і стає більш конкурентоспроможним у сучасному цифровому світі.

1.2 Класифікація хмарних сервісів

Хмарні сервіси сьогодні є важливим елементом сучасної інформаційної інфраструктури підприємств та організацій. Вибір моделі хмарних сервісів має визначальний вплив на ефективність, безпеку та вартість використання ресурсів. Основними параметрами класифікації таких сервісів є модель надання послуг та модель розгортання інфраструктури.

1.2.1 Моделі надання хмарних послуг

Хмарні сервіси поділяються на три основні моделі: інфраструктура як сервіс (IaaS), платформа як сервіс (PaaS) і програмне забезпечення як сервіс (SaaS). Ці моделі відрізняються між собою ступенем контролю, який отримує кінцевий користувач, і рівнем відповідальності постачальника.

Інфраструктура як сервіс (IaaS)

У цій моделі користувач отримує віртуальні сервери, сховища та мережеве обладнання, з якими може працювати майже як із власними. Він сам керує операційною системою, програмами та налаштуваннями безпеки. Постачальник

відповідає лише за «залізо» і мережу, щоб усе працювало без збоїв. Головна перевага — це гнучкість: можна швидко змінювати кількість ресурсів залежно від потреб.

Приклади:

Amazon Elastic Compute Cloud (EC2)

Microsoft Azure Virtual Machines

Google Compute Engine

Платформа як сервіс (PaaS)

Модель PaaS надає середовище, в якому можна створювати, тестувати та запускати додатки без турбот про інфраструктуру. Користувач відповідає лише за сам додаток і його налаштування, а все інше — операційні системи, бази даних, сервери — забезпечує провайдер. Такий варіант особливо зручний для команд розробників, які хочуть зосередитися на написанні коду, а не на налаштуванні серверів чи оновленнях.

У моделі SaaS користувач просто працює з готовою програмою через Інтернет — нічого не потрібно встановлювати на комп’ютер. Усі технічні речі, як-от оновлення, налаштування чи підтримка, виконує сам провайдер. Це дуже зручно для малого бізнесу та звичайних користувачів, яким важливо, щоб усе працювало «з коробки» без зайвих складнощів.

1.2.2 Моделі розгортання хмарних сервісів

Розгортання хмарних обчислень здійснюється за кількома ключовими моделями: публічна, приватна, гібридна та мультихмара.

У публічній хмарі вся інфраструктура належить зовнішньому провайдеру, і користувачі отримують доступ до ресурсів через Інтернет. Це найпоширеніший варіант, бо він швидко впроваджується, легко масштабується і має невелику стартову вартість. Але є й мінуси — користувач майже не контролює технічну частину, існують ризики для конфіденційності даних, а також залежність від

надійності самого провайдера.Приватна хмара використовується виключно однією організацією і може бути розміщена як у власному дата-центрі компанії, так і у спеціалізованого хостинг-провайдера. Вона забезпечує максимальний контроль за ресурсами, високий рівень безпеки та відповідність внутрішнім стандартам компанії. Головні недоліки — висока вартість впровадження, необхідність утримання штатних фахівців та складність масштабування ресурсів.

Гібридна хмара поєднує кращі сторони приватної та публічної. Конфіденційні дані зберігаються локально, у власній інфраструктурі, а менш важливі сервіси працюють у публічній хмарі. Це дає змогу зручно керувати ресурсами, економити кошти та підвищити надійність роботи. Але є і мінуси — така система складніша в управлінні й потребує правильної інтеграції між різними середовищами.

У цій моделі використовують відразу кілька публічних хмар від різних провайдерів. Це допомагає уникнути залежності від одного постачальника, обрати найвигідніші умови та зробити систему більш надійною завдяки резервуванню. Але є й складності — потрібно керувати кількома платформами одночасно, правильно їх інтегрувати і слідкувати за єдиною політикою безпеки.

1.2.3 Додаткові спеціалізовані моделі

Крім основних моделей, існують також спеціалізовані сервіси, такі як:

Desktop as a Service (DaaS) — віртуалізація робочих столів.

Backend as a Service (BaaS) — забезпечення бекенд-функціоналу для мобільних додатків.

Function as a Service (FaaS) — запуск програмного коду без управління серверами (AWS Lambda, Google Cloud Functions).

1.3 Переваги та недоліки хмарних технологій

Хмарні технології швидко набули популярності, адже мають багато переваг як для компаній, так і для звичайних користувачів. Але, разом із плюсами, вони несуть і певні ризики, про які теж варто пам’ятати перед тим, як почати їх використовувати.

1.3.1 Переваги хмарних технологій

Завдяки хмарним технологіям суттєво змінився підхід до ІТ як у бізнесі, так і в освіті, держсфері та навіть у звичайному житті. Саме їхні зручності й вигоди пояснюють, чому такі рішення так стрімко поширюються по всьому світу.

1) Економія коштів та менші витрати на інфраструктуру. Один із головних плюсів хмарних обчислень — це помітне зниження витрат. Компаніям більше не потрібно купувати дорогі сервери, сховища чи мережеве обладнання, а також витрачатися на електрику, обслуговування й охолодження. Усе це бере на себе провайдер. Платити потрібно тільки за те, що реально використовується — за моделлю «pay-as-you-go».

2) Гнучкість і легке масштабування. Хмарні сервіси дуже зручні тим, що ресурси можна швидко збільшити або зменшити залежно від потреб. Компаніям не треба чекати на закупівлю чи встановлення нового обладнання — усе налаштовується онлайн і займає мінімум часу.

3) Надійний доступ і резервування даних. Хмарні сервіси працюють стабільно завдяки тому, що дані зберігаються одразу в кількох дата-центрах. Якщо один із них виходить з ладу — нічого страшного, інформація лишається доступною. Це важливо для бізнесу, бо дозволяє уникнути простоїв і втрати даних.

4) Географічна мобільність та віддалений доступ. Однією з ключових переваг хмарних технологій є можливість працювати з ресурсами з будь-якої точки світу, де є доступ до Інтернету.

5) Автоматизація рутинних процесів обслуговування. Хмарні провайдери беруть на себе завдання, пов’язані з технічним обслуговуванням інфраструктури, автоматичними оновленнями програмного забезпечення, налаштуванням безпеки, резервним копіюванням та моніторингом систем.

6) Покращена інформаційна безпека (за умов коректного налаштування). Професійні хмарні провайдери інвестують значні ресурси у забезпечення високого рівня безпеки, використовуючи передові технології шифрування, багатофакторну автентифікацію, антивірусний захист, системи виявлення вторгнень (IDS), системи запобігання витокам даних (DLP), що часто є більш потужними та сучасними, ніж можливості окремих компаній.

7) Швидкість впровадження нових технологій. Хмарні сервіси дозволяють компаніям надзвичайно швидко запускати нові програмні рішення, сервіси та додатки. Відсутність необхідності купувати й налаштовувати обладнання значно скорочує час виходу продукту на ринок, надаючи підприємствам суттєві конкурентні переваги та допомагаючи швидше реагувати на зміни ринкових умов.

8) Краще командне співробітництво. Хмарні сервіси допомагають працівникам зручно працювати разом — можна одночасно редагувати документи, ділитися файлами, користуватись спільними базами знань і швидко обмінюватися інформацією. Усе це відбувається в реальному часі, навіть якщо люди працюють з різних міст чи країн.

9) Екологічна ефективність та зменшення впливу на навколишнє середовище. Консолідація ресурсів у великих дата-центрах дозволяє ефективніше використовувати енергоресурси та знижувати вплив на екологію.

10) Доступ до новітніх технологій. Завдяки хмарним сервісам компанії можуть користуватись сучасними технологіями — такими як штучний інтелект, великі дані, блокчейн чи Інтернет речей (IoT). І все це — без великих витрат на обладнання чи найм дорогих спеціалістів. Усе вже налаштовано і готове до використання.

11) Відповідність сучасним регуляторним вимогам. Великі хмарні провайдери забезпечують відповідність міжнародним та національним стандартам захисту інформації (GDPR, ISO 27001, HIPAA).

1.3.2 Недоліки та ризики хмарних технологій

Попри всі переваги, хмарні технології мають і свої мінуси. Їх використання пов’язане з певними ризиками, про які не можна забувати. Щоб правильно впровадити хмарні рішення та уникнути проблем у майбутньому, важливо заздалегідь враховувати ці фактори і добре зважувати рішення.

1) Залежність від Інтернету. Один із головних мінусів хмарних рішень — це повна залежність від стабільного з’єднання. Якщо Інтернет працює повільно або з перебоями, доступ до сервісів може серйозно ускладнитися. У результаті — зниження продуктивності, затримки в роботі, а іноді й повна зупинка важливих процесів.

2) Ризики для конфіденційності та безпеки. Передаючи дані сторонньому провайдеру, компанія частково втрачає над ними контроль. Навіть якщо це надійний сервіс, завжди існує ймовірність витоку або несанкціонованого доступу. Це особливо критично для сфер, де обробляються чутливі дані — наприклад, у фінансах, медицині чи державному секторі.

3) Втрата контролю над IT-інфраструктурою. При використанні хмарних сервісів, особливо моделей SaaS або публічних хмар, компанії значною мірою втрачають контроль над базовою IT-інфраструктурою.

4) Складність перенесення даних. Перехід на хмару або повернення до локальної інфраструктури — справа непроста. Це може займати багато часу, вимагати залучення спеціалістів і коштувати недешево. Часто виникають проблеми з сумісністю між різними провайдерами або нестачею єдиних стандартів перенесення, що ще більше ускладнює процес.

5) Залежність від одного провайдера (Vendor lock-in). Якщо компанія використовує інструменти й сервіси лише одного постачальника, з часом може виникнути ситуація, коли перейти на іншу платформу буде складно й дорого. Це створює залежність, яка обмежує свободу вибору в майбутньому.

6) Юридичні та регуляторні ризики. Компанії, які користуються послугами міжнародних хмарних провайдерів, можуть зіткнутися з проблемами дотримання законів — як своїх країн, так і міжнародних стандартів, наприклад GDPR або HIPAA. У різних країнах правила зберігання та обробки персональних даних можуть сильно відрізнятися, і це іноді призводить до юридичних труднощів і навіть штрафів.

7) Можливе зростання витрат з часом. Хоча на старті хмарні сервіси здаються вигідними, у довгостроковій перспективі витрати можуть сильно зрости. Це стосується передусім компаній, які постійно використовують велику кількість ресурсів. У результаті — щомісячні платежі можуть стати вищими, ніж витрати на власну інфраструктуру.

У першому розділі дипломної роботи були розглянуті основи хмарних обчислень: що це таке, як вони працюють, які існують моделі надання послуг і варіанти розгортання. Також було проаналізовано ключові переваги та недоліки цих технологій, що дозволяє краще зрозуміти їхню роль у сучасному IT-середовищі.

Проведений аналіз показав, що хмарні технології є однією з найважливіших інновацій у сфері IT. Вони змінюють підхід до управління ресурсами — роблять його гнучкішим, ефективнішим і вигіднішим з точки зору витрат. Завдяки хмарним сервісам організації можуть скоротити початкові інвестиції у створення власної IT-інфраструктури та значно зменшити витрати на її підтримку.

Підсумовуючи проведений аналіз, можна зробити висновок, що хмарні технології є перспективним та доцільним вибором для багатьох сучасних компаній. Проте, щоб повністю використати їхній потенціал, необхідно ретельно оцінити потреби організації, розуміти особливості різних моделей надання та розгортання сервісів, а

також грамотно управляти пов’язаними ризиками. Вибір оптимального варіанту повинен базуватись на комплексному аналізі технічних, економічних і безпекових факторів. Це дозволить отримати максимум користі від хмарних обчислень і підсилити конкурентоспроможність організації.

2 АНАЛІЗ ЗАГРОЗ ТА ВРАЗЛИВОСТЕЙ В ХМАРНИХ СЕРЕДОВИЩАХ

2.1 Основні загрози інформаційній безпеці в хмарних обчисленнях

Із розвитком хмарних технологій зростає й кількість загроз для інформаційної безпеки. Це пов’язано зі способом зберігання, передачі та обробки даних у розподіленому середовищі. Тому, щоб надійно захистити інформацію, важливо розуміти найпоширеніші та найактуальніші загрози, з якими стикаються як користувачі, так і провайдери хмарних сервісів.

Серед основних загроз інформаційній безпеці у хмарних середовищах можна виокремити такі:

1) Несанкціонований доступ до інформації (Unauthorized Access)

Одна з найтиповіших проблем у хмарних системах — це сторонній доступ до облікових записів. Таке трапляється, коли паролі надто прості, автентифікація не двоетапна, або коли працівники самі втрачають контроль над логінами. У результаті — конфіденційна інформація може опинитися у чужих руках, що не лише загрожує безпеці, а й може серйозно зіпсувати репутацію організації.

2) Перехоплення та витік інформації (Data Breach)

Оскільки хмарні сервіси працюють через Інтернет, дані постійно передаються мережею — і це створює ризик їхнього перехоплення. Якщо з’єднання не захищене або дані не шифруються, зловмисники можуть скористатися вразливостями та отримати доступ до важливої інформації. Такі витоки можуть статися навіть через банальну технічну недбалість.

3) Втрата даних (Data Loss)

Втрата даних — одна з найнеприємніших загроз у хмарному середовищі. Причини можуть бути різні: збій обладнання, помилка в програмі, випадкове видалення файлів працівником або навіть стихійне лихо. Особливу небезпеку

становлять атаки вірусів-вимагачів (ransomware), які блокують доступ до інформації та вимагають викуп.

4) Внутрішні загрози (Insider Threats)

Не всі загрози приходять ззовні — іноді джерелом проблем можуть бути самі працівники або адміністратори, які мають доступ до важливої інформації. Це може бути як випадкова помилка, так і свідомі дії. У хмарних сервісах ситуація ще складніша: частина даних зберігається у сторонніх компаній, тож коло осіб, які можуть щось побачити або змінити, суттєво розширюється.

5) Атаки типу «відмова в обслуговуванні» (DDoS)

Хмарні платформи часто стають мішенню DDoS-атак — це коли зловмисники навмисно перевантажують систему великою кількістю запитів, щоб вона перестала працювати. У результаті користувачі можуть тимчасово втратити доступ до сервісів, що викликає простої й порушує роботу бізнесу.

6) Компрометація інтерфейсів управління (API vulnerabilities)

У хмарних платформах широко застосовуються API — спеціальні інтерфейси, через які різні частини системи взаємодіють між собою. Якщо ці інтерфейси погано захищені, хакери можуть скористатися цим, щоб отримати доступ до налаштувань, змінити правила безпеки або навіть повністю зламати систему.7) Недоліки багатокористувацької архітектури (Multi-Tenancy Issues)

У хмарних сервісах часто кілька клієнтів користуються одними й тими самими ресурсами — це називається мультиорендою. Якщо десь допущено помилку в налаштуваннях або в коді, може вийти так, що один користувач побачить дані іншого. Для конфіденційної інформації це — серйозна загроза.8) Неналежна конфігурація безпеки (Security Misconfiguration)

Частою причиною порушень інформаційної безпеки є неправильне налаштування хмарних сервісів. Помилки, допущені при налаштуванні системи,

можуть дозволити зловмисникам легко отримати доступ до незахищених ресурсів, баз даних чи сховищ даних.

9) Вразливості віртуалізації (Virtualization Vulnerabilities)

Щоб ефективно розподіляти ресурси, хмарні сервіси використовують віртуалізацію — тобто розділяють один фізичний сервер на кілька віртуальних машин. Але якщо в самій технології є вразливість, хакер може «вийти за межі» своєї віртуальної машини та отримати доступ до інших систем або навіть до всього фізичного сервера.

10) Шкідливе програмне забезпечення (Malware)

Віруси, шпигунські програми та інше шкідливе ПЗ можуть потрапити в хмару з заражених комп’ютерів користувачів або через слабкі місця в системі. Якщо така програма «оселиться» у хмарному середовищі, зловмисники можуть почати красти дані, видаляти файли або запускати інші атаки.

Отже, хоча хмарні обчислення дають багато переваг, вони водночас приносять і нові загрози для безпеки даних. Щоб ефективно з ними впоратись, спочатку потрібно добре розуміти, з чим саме можуть виникнути проблеми. Глибокий аналіз таких загроз допомагає побачити слабкі місця, правильно розставити пріоритети та обрати дієві способи захисту інформації в хмарному середовищі.

2.2 Типові вразливості хмарних сервісів

Хмарні технології відкривають нові можливості, але разом із ними приносять і свої слабкі місця. Зловмисники можуть використати ці вразливості, щоб отримати доступ до даних або зламати систему. Тому, перш ніж говорити про захист, важливо розібратися, де саме ховаються типові проблеми в хмарних сервісах.

Серед найбільш поширених типових вразливостей хмарних середовищ можна виокремити такі:

1) Недостатній контроль доступу (Broken Access Control)

Проблеми з автентифікацією та авторизацією часто виникають тоді, коли ці механізми налаштовані неправильно або надто спрощено. У такому випадку зловмисники можуть обійти перевірку доступу й дістатися до чужих даних або ресурсів. Особливо це стосується API та веб-консолей, через які керують хмарною інфраструктурою.

2) Неправильна конфігурація хмарного середовища (Cloud Misconfiguration)

Багато проблем у хмарі виникає просто через людську неуважність або поспіх. Наприклад, хтось залишає відкритий доступ до бази даних, не вмикає шифрування, або взагалі використовує стандартні налаштування безпеки "за замовчуванням". Усе це може легко призвести до витоку інформації або стати «вхідними воротами» для атаки.

3) Недоліки ізоляції ресурсів (Resource Isolation Failures)

У хмарі часто кілька клієнтів користуються одним фізичним сервером — кожен у своїй віртуальній машині чи контейнері. Але якщо між ними немає чіткої межі, зловмисник може пробратися з однієї віртуалки в іншу. Такі «дірки» в ізоляції створюють серйозну загрозу, бо одна вразлива машина може поставити під ризик усіх інших на тому самому сервері.

4) Вразливості програмних інтерфейсів (API Vulnerabilities)

API — це те, через що програми «спілкуються» між собою, і в хмарних сервісах вони грають ключову роль. Але якщо розробники не подбали про перевірку введених даних або чіткий контроль доступу, можуть виникати серйозні проблеми. Через такі «дірки» зловмисники отримують доступ до чужої інформації або навіть запускають небезпечні команди.

5) Вразливості програмного забезпечення віртуалізації (Virtualization Software Vulnerabilities)

Щоб поділити один фізичний сервер між кількома користувачами, хмарні провайдери використовують гіпервізори — спеціальні програми, які керують

віртуальними машинами. Але якщо в самому гіпервізорі є помилка, зловмисник може вибратись зі своєї віртуалки й дістатись до інших або навіть отримати контроль над усім фізичним сервером.

6) Недостатня захищеність даних під час передачі (Insecure Data Transfer)

Якщо дані між користувачем і хмарним сервісом не шифруються або шифрування налаштовано неправильно, їх легко можуть перехопити. Це особливо небезпечно, коли йдеться про особисту інформацію, фінансові операції чи інші чутливі дані — усе це може потрапити в руки зловмисників.

7) Недостатня прозорість і контроль з боку провайдера (Limited Provider Transparency)

Не всі провайдери хмарних сервісів відкрито розповідають, як саме вони захищають дані. Через це компаніям важко оцінити, наскільки сервіс безпечний і чи відповідає він їхнім вимогам. Така «непрозорість» може стати серйозним ризиком, особливо коли йдеться про важливу або конфіденційну інформацію.

8) Незахищеність системи зберігання даних (Insecure Data Storage)

Часто безпеці збережених у хмарі даних приділяють недостатньо уваги. Якщо не вмикати шифрування, залишити відкритий доступ до сховищ або зберігати резервні копії без захисту — усе це відкриває двері для витоку або втрати важливої інформації.

9) Недостатній захист від DDoS-атак (Inadequate DDoS Protection)

Не всі хмарні сервіси добре захищені від DDoS-атак. Якщо таких механізмів немає або вони слабкі, навіть невелика атака може «покласти» сервіс або суттєво уповільнити його роботу. В результаті користувачі можуть тимчасово втратити доступ до своїх даних і ресурсів.

10) Людський фактор (Human Factor)

Людський фактор залишається однією з головних причин проблем із безпекою. Адміністратор може щось неправильно налаштувати, користувач — випадково

видалити важливі дані або не так скористатись функцією безпеки. Такі помилки, на перший погляд дрібні, часто призводять до серйозних наслідків для всієї організації.

Як показує аналіз, вразливості хмарних сервісів можуть виникати з різних причин — від технічних недоліків до банальних помилок користувачів. Щоб зменшити ризики, потрібно регулярно перевіряти налаштування безпеки, оновлювати системи, обмежувати доступ до важливих даних і навчати персонал, як правильно користуватись хмарними сервісами. Розуміння типових слабких місць — це перший і обов'язковий крок до створення надійної та безпечної хмарної інфраструктури.

2.3 Моделі загроз і методики оцінювання ризиків

Щоб справді ефективно захищати дані в хмарі, недостатньо просто знати про загрози й вразливості. Потрібно ще вміти їх моделювати та оцінювати пов'язані з ними ризики. Саме моделі загроз і спеціальні методики аналізу ризиків допомагають побачити слабкі місця заздалегідь і вибудувати чітку та дієву стратегію захисту інформації.

2.3.1 Поняття моделі загроз та її значення

Модель загроз — це спосіб у структурованій формі описати, звідки може прийти небезпека для інформаційної системи. Вона допомагає побачити, хто може атакувати систему, яким шляхом, де є слабкі місця і що може статися в разі успішної атаки. Основна ідея моделювання — знайти всі потенційні точки ризику й заздалегідь продумати, як захиститися або зменшити можливі наслідки.

2.3.2 Основні методики моделювання загроз

Сьогодні для моделювання загроз використовують кілька перевірених підходів. Найпопулярніші серед них — це STRIDE, DREAD, OCTAVE та так звані

дерева атак (Attack Trees). Кожна з цих методик має свій підхід до аналізу ризиків і допомагає по-своєму виявляти та описувати потенційні загрози в інформаційних системах.

Методика STRIDE була розроблена компанією Microsoft і включає такі категорії загроз: spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege

STRIDE допомагає класифікувати загрози, а от методика DREAD дозволяє їх оцінити. Цей підхід базується на кількісному аналізі ризиків і допомагає зрозуміти, наскільки серйозною є та чи інша загроза. Оцінювання проводиться за п’ятьма критеріями: damage, reproducibility, affected, exploitability, discoverability

Кожен параметр оцінюється за шкалою від 0 до 10, після чого визначається загальний рівень ризику.

Методологія OCTAVE (скорочено від Operationally Critical Threat, Asset, and Vulnerability Evaluation) підходить до безпеки з позиції бізнесу. Вона допомагає зрозуміти, які саме активи організації є критично важливими — наприклад, фінансові системи, дані клієнтів або внутрішні процеси — і які загрози можуть їм зашкодити. На основі цього формується оцінка ризиків і визначаються кроки для їх мінімізації. Такий підхід особливо ефективний у великих компаніях, де потрібно координувати IT-безпеку з масштабною інфраструктурою та бізнес-завданнями.

Метод дерев атак (Attack Trees) дозволяє візуально змоделювати, як може бути реалізована атака — від її основної мети до конкретних кроків, які може зробити зловмисник. Така схема допомагає краще зрозуміти можливі варіанти дій з боку атакуючого, порівняти сценарії між собою і виявити ті з них, які становлять найбільшу небезпеку чи є найбільш імовірними.

2.3.3 Методики оцінювання ризиків у хмарних обчисленнях

Після того як потенційні загрози визначено та змодельовано, наступним кроком стає оцінювання ризиків. Існує кілька підходів до цього процесу, серед яких найпоширенішими є: якісна оцінка, кількісна оцінка та змішаний підхід. Кожен із них має свої переваги й застосовується залежно від специфіки завдань, доступних даних та рівня деталізації, який потрібно досягти.

Якісна оцінка ризиків базується переважно на експертних судженнях. У цьому підході ризики класифікуються за рівнем імовірності та серйозності наслідків — наприклад, як низькі, середні або високі. Це дозволяє швидко зорієнтуватися, які загрози є найбільш критичними, без залучення складних формул чи математичних моделей.

Кількісна оцінка ризиків використовує точні цифри, статистику та математичні моделі. У цьому підході ризики вимірюються у грошовому або іншому числовому вираженні. Зокрема, застосовують такі показники, як ALE (Annualized Loss Expectancy) — річний очікуваний збиток, ARO (Annualized Rate of Occurrence) — частота виникнення загрози протягом року, та SLE (Single Loss Expectancy) — середні втрати від одного інциденту. Така оцінка дозволяє більш точно прогнозувати можливі втрати й планувати витрати на заходи безпеки.

Змішаний (гібридний) підхід поєднує переваги якісного та кількісного оцінювання ризиків. Такий підхід дозволяє спочатку швидко зорієнтуватися в основних загрозах (як у якісній моделі), а потім — деталізувати окремі ризики за допомогою цифр і розрахунків. Це забезпечує більш збалансовану та обґрунтовану оцінку і часто вважається найоптимальнішим варіантом для реальних умов.

Ефективний захист у хмарі потребує аналізу загроз і ризиків. Методики типу STRIDE та DREAD допомагають виявити загрози й визначити пріоритети безпеки.

3 МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В ХМАРНИХ ОБЧИСЛЕННЯХ

3.1 Криптографічні методи захисту інформації у хмарних обчисленнях

Криптографія — один з найнадійніших способів захисту даних у хмарі. Вона забезпечує конфіденційність, цілісність і автентичність, знижуючи ризики несанкціонованого доступу, витоку або підміни даних під час зберігання й передачі.

Основними криптографічними підходами, що застосовуються для захисту інформації в хмарних обчисленнях, є:

1) Симетричне шифрування

Симетричне шифрування передбачає застосування одного секретного ключа для шифрування та розшифрування даних. Такий підхід відзначається високою швидкістю роботи алгоритмів і відносною простотою реалізації, що робить його популярним у багатьох системах захисту інформації.

Найбільш популярними алгоритмами симетричного шифрування, що активно використовуються в хмарних середовищах, є:

AES — це сучасний стандарт шифрування, який надійно захищає дані. Його часто використовують у популярних хмарних сховищах, як Amazon S3 чи Google Cloud Storage, щоб гарантувати безпеку інформації клієнтів.

DES — це старіший алгоритм шифрування, який вже вважається застарілим, але іноді досі використовують у системах з менш високими вимогами до безпеки.

Triple DES (3DES) — це вдосконалена версія DES, яка підвищує рівень безпеки. Проте зараз поступається за надійністю і швидкістю більш сучасному AES.

2) Асиметричне шифрування (шифрування з відкритим ключем)

Асиметричне шифрування працює з двома ключами — відкритим і приватним. Відкритий ключ використовують для шифрування даних, а приватний — для їх розшифрування. На рисунку 3.1 показано, як відбувається захищена передача

інформації в хмарне середовище. Головна перевага такого методу — надійніший захист, особливо коли дані передаються через відкриті мережі.

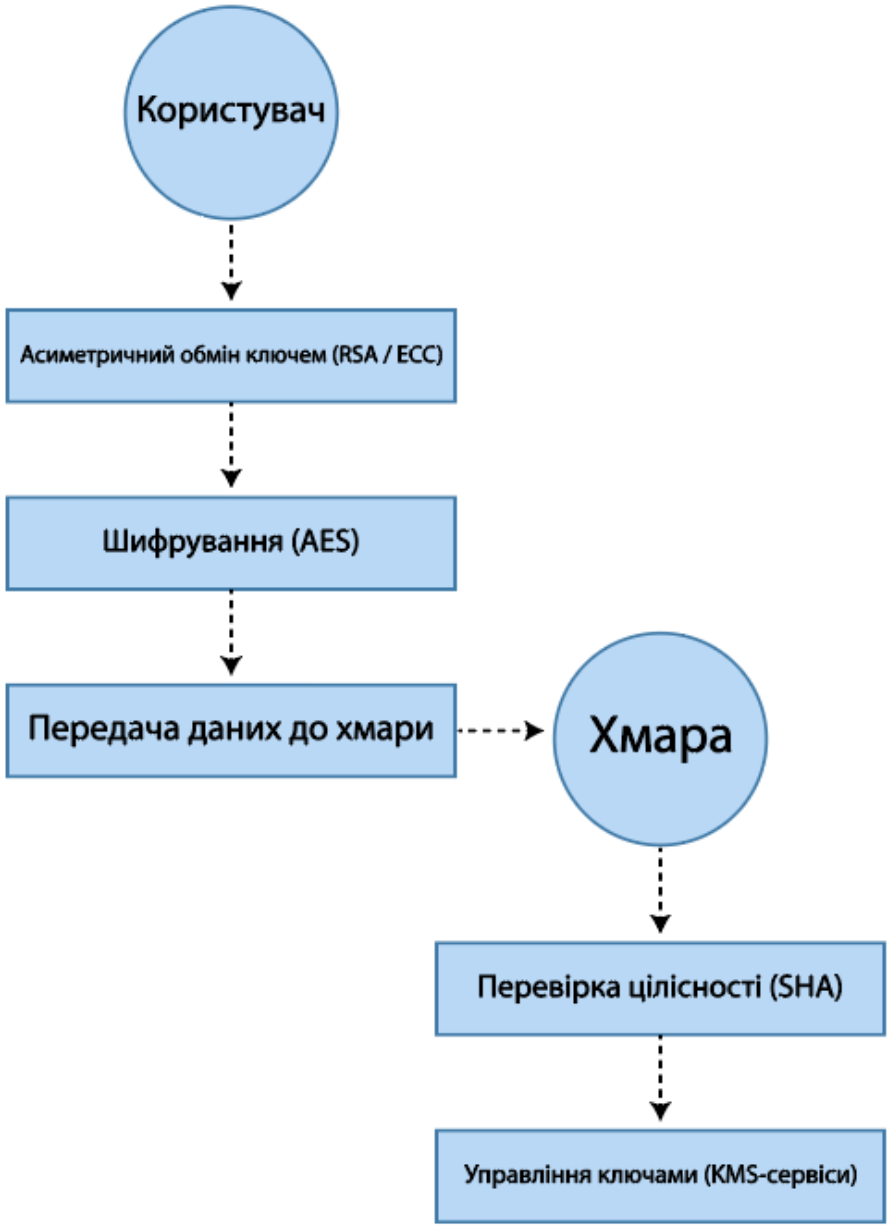

Рисунок 3.1 – Схема криптографічного захисту в хмарі

До найбільш поширених алгоритмів асиметричного шифрування належать:

RSA (Rivest–Shamir–Adleman) – найбільш поширений алгоритм для захисту даних, цифрових підписів та сертифікатів безпеки.

ECC (Elliptic Curve Cryptography) — це алгоритм шифрування, який працює на основі математичних властивостей еліптичних кривих. Його головна перевага — коротші ключі порівняно з RSA, але при цьому він гарантує високий рівень безпеки. Це особливо корисно для хмарних ресурсів, де потужностей для обчислень зазвичай не так багато, а інформацію потрібно захищати надійно.

3) Гібридні методи шифрування

Гібридні методи поєднують переваги двох типів шифрування: симетричного та асиметричного. Суть проста — спочатку використовують асиметричний алгоритм, щоб безпечно передати ключ для симетричного шифрування. А потім вже цим ключем шифрується сама інформація. Завдяки такій схемі можна ефективно та без зайвих витрат ресурсів захистити великі об'єми даних.

Прикладом такого підходу є протокол TLS (Transport Layer Security), який широко використовується для забезпечення захищеного обміну даними у хмарних середовищах.

4) Хеш-функції та забезпечення цілісності даних

Хеш-функції використовують, щоб переконатися, що інформацію ніхто не змінював. Вони створюють такий собі цифровий «відбиток», який буде абсолютно унікальним для конкретних даних. Якщо дані навіть трішечки зміняться, відбиток теж зміниться, і це одразу буде помітно. Серед популярних алгоритмів хешування можна виділити:

SHA-256, SHA-384, SHA-512 (Secure Hash Algorithm) – сучасні алгоритми хешування, які забезпечують високий рівень захисту інформації від несанкціонованих змін.

MD5 (Message Digest Algorithm) – застарілий алгоритм, але іноді ще використовується для перевірки цілісності файлів, хоча не рекомендується для критичних завдань.

5) Цифровий підпис

Цифровий підпис потрібен, щоб переконатися, що інформація справді походить саме від того, хто її надіслав, і що її ніхто не змінював під час передачі. Для створення такого підпису зазвичай використовують комбінацію двох технологій: асиметричного шифрування і хешування. Це допомагає гарантувати справжність та цілісність будь-яких цифрових документів або повідомлень.

У хмарних сервісах цифровий підпис активно застосовується при роботі з API, веб-застосунками, договорами та іншими конфіденційними документами.

6) Управління ключами шифрування (Key Management)

Однією з найважливіших частин захисту інформації у хмарі є грамотне управлення ключами шифрування. Сьогодні провайдери хмарних сервісів спеціально для цього створили свої системи управління ключами — наприклад, AWS Key Management Service (KMS), Google Cloud KMS та Azure Key Vault. Ці сервіси дозволяють зберігати ключі у безпеці, регулярно їх оновлювати та зручно контролювати доступ до них, що значно посилює загальний рівень захищеності даних (таблиця 3.1).

Таблиця 3.1 – Переваги та недоліки основних шифрів

Метод	Призначення	Переваги	Недоліки
AES	Симетричне шифрування	Швидке, стійке	Не підходить для відкритих мереж
RSA	Асиметричне шифрування	Безпечна передача ключів	Повільне
ECC	Асиметричне шифрування на еліптичних кривих	Менші ключі, висока ефективність	Складність реалізації
TLS	Гібридне шифрування	Стандарт для веб-з'єднань	Залежить від налаштування

Можна зробити висновок, що криптографічні методи — це основа безпеки в хмарних середовищах. Саме вони допомагають зберегти конфіденційність даних, гарантувати їхню цілісність і впевнитися в справжності джерела. Але для того, щоб усе це дійсно працювало, важливо не просто використовувати шифрування, а ще й правильно обрати алгоритми, добре захищати ключі й грамотно налаштувати сервіси, які для цього пропонують хмарні провайдери.

3.2 Автентифікація, авторизація та контроль доступу

Одними з ключових елементів безпеки в хмарних середовищах є автентифікація, авторизація та контроль доступу. Саме ці механізми визначають, хто саме може заходити в систему, до яких ресурсів він має доступ і що саме йому дозволено з цими ресурсами робити. Від того, наскільки чітко та грамотно вони реалізовані, залежить не лише зручність роботи користувачів, а й загальний рівень захисту всієї хмарної інфраструктури

3.2.1 Автентифікація у хмарних середовищах

Автентифікація – це процес перевірки особи користувача або пристрою, що намагається отримати доступ до інформаційних ресурсів. Основними методами автентифікації, які активно використовуються у хмарних обчисленнях, є:

Однофакторна автентифікація (SFA) — це коли для входу використовується лише один засіб підтвердження особи, зазвичай пароль. З одного боку, це просто і зручно, але з іншого — досить небезпечно. Пароль можна легко вгадати, вкрасти або перехопити, тому такий спосіб захисту вважається одним із найменш надійних.

Багатофакторна автентифікація — це коли для входу в систему недостатньо одного лише пароля. Наприклад, після введення пароля потрібно ще ввести код із SMS, скористатися апаратним токеном чи підтвердити особу відбитком пальця. Завдяки такій схемі зловмиснику доведеться мати одночасно кілька різних речей

(пароль, телефон або токен, біометричні дані), і це значно ускладнює будь-яку спробу несанкціонованого доступу.

Біометрична автентифікація – використовує фізичні характеристики користувача (відбитки пальців, розпізнавання обличчя, голосу тощо). Стає дедалі популярнішою завдяки простоті та високому рівню безпеки. На рисунку 3.2 зображена схема авторизації та автентифікації користувачів в хмарному середовищі.

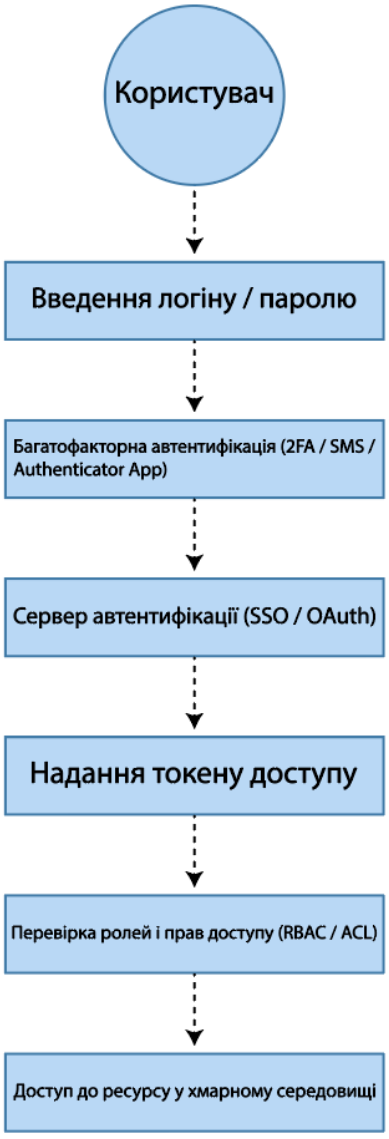

Рисунок 3.2 – Схема автентифікації та авторизації у хмарному середовищі

3.2.2 Авторизація у хмарних сервісах

Авторизація — це етап, який настає після автентифікації, коли система вже «впевнена», хто саме перед нею. Тут визначається, до чого саме цей користувач має доступ: які дані він може переглядати, що редагувати, а що йому взагалі заборонено. Важливими підходами до авторизації у хмарних сервісах є:

RBAC (Role-Based Access Control) – контроль доступу на основі ролей, при якому доступ до ресурсів надається відповідно до ролі, яку виконує користувач у компанії. Це дозволяє чітко й централізовано керувати дозволами, зменшуючи ймовірність помилок конфігурації доступу.

ABAC (Attribute-Based Access Control) – контроль доступу на основі атрибутів користувача, таких як місце розташування, час доступу, тип пристрою тощо. Це дозволяє реалізувати більш гнучкі й детальні політики безпеки.

MAC (Mandatory Access Control) – обов'язковий контроль доступу, що використовується в суворих середовищах з високими вимогами до безпеки. В цьому випадку права доступу визначаються адміністратором централізовано й не можуть бути змінені самим користувачем.

3.2.3 Контроль доступу (Access Control)

Контроль доступу забезпечує захист ресурсів шляхом обмеження або надання доступу користувачам відповідно до визначених політик. Для реалізації контролю доступу у хмарних середовищах використовуються:

Політики IAM (Identity and Access Management) – системи управління ідентифікацією та доступом, що дозволяють створювати та контролювати дозволи користувачів. Типові приклади таких систем – AWS IAM, Azure AD та Google Cloud IAM.

Системи єдиного входу (Single Sign-On, SSO) – дозволяють користувачам використовувати єдиний набір облікових даних для доступу до багатьох різних

сервісів, що підвищує зручність використання та знижує ризик компрометації облікових записів.

Zero Trust Model (модель нульової довіри) – концепція, яка базується на припущенні, що всі користувачі, навіть ті, що знаходяться всередині мережі, не є повністю довіреними. Це змушує застосовувати перевірку автентичності на всіх етапах доступу до ресурсів.

3.3 Моніторинг, аудит та політики безпеки у хмарних середовищах

Однією з основних складових інформаційної безпеки в хмарних середовищах є налагоджений моніторинг, регулярний аудит безпеки та чітко визначені політики захисту. Ці заходи дають змогу своєчасно виявляти можливі загрози, контролювати відповідність стандартам і швидко реагувати на інциденти, забезпечуючи таким чином надійний захист даних.

3.3.1 Моніторинг у хмарних середовищах

Моніторинг є важливим інструментом для виявлення підозрілих дій, інцидентів безпеки та аномальної поведінки в хмарному середовищі. Основні напрями моніторингу включають:

Моніторинг подій безпеки (Security Event Monitoring) – забезпечує контроль над подіями, що можуть свідчити про несанкціоновані спроби доступу, злам або атаки типу DDoS.

Моніторинг доступу до ресурсів (Access Monitoring) – контроль активності користувачів для виявлення незвичних шаблонів поведінки або несанкціонованих спроб доступу.

Моніторинг конфігурації (Configuration Monitoring) – контроль змін у конфігурації хмарних ресурсів для попередження випадкових або зловмисних змін налаштувань безпеки.

Серед популярних рішень для моніторингу можна виокремити такі:

AWS CloudWatch, Google Cloud Monitoring, Azure Monitor – стандартні інструменти хмарних провайдерів для моніторингу активності та ресурсів.

SIEM-системи (Security Information and Event Management) – комплексні рішення, що дозволяють аналізувати події безпеки з різних джерел (наприклад, Splunk, IBM QRadar, Microsoft Sentinel).

3.3.2 Аудит безпеки у хмарних середовищах

Регулярний аудит дає змогу оцінити ефективність системи інформаційної безпеки, виявити недоліки у налаштуваннях, перевірити відповідність встановленим вимогам та оперативно усунути виявлені проблеми.

До основних завдань аудиту безпеки входять:

Перевірка відповідності політикам та стандартам безпеки.

Виявлення потенційних уразливостей і ризиків.

Аналіз ефективності впроваджених заходів безпеки.

Розробка рекомендацій для покращення безпеки.

Аудит безпеки хмарних сервісів проводиться за допомогою спеціалізованих інструментів, таких як:

AWS Trusted Advisor, Google Cloud Security Command Center – сервіси, що дозволяють автоматично оцінити відповідність налаштувань рекомендаціям безпеки.

Інструменти penetration testing (тестування на проникнення) – для активного виявлення вразливостей шляхом симуляції атак.

3.3.3 Політики безпеки у хмарних середовищах

Політики безпеки — це офіційні документи, що визначають правила та процедури для забезпечення інформаційної безпеки. В умовах хмарних середовищ вони мають враховувати особливості роботи з ресурсами, механізми контролю

доступу, шифрування даних, а також відповідність регуляторним вимогам і стандартам.

Типові політики безпеки, що мають бути впроваджені у хмарних середовищах, включають:

Політика управління доступом (Access Control Policy) – регулює права доступу та обов’язки користувачів.

Політика шифрування даних (Data Encryption Policy) – визначає стандарти використання криптографічних методів захисту.

Політика реагування на інциденти (Incident Response Policy) – описує процедури дій персоналу при виникненні інцидентів інформаційної безпеки.

Політика резервного копіювання (Backup and Recovery Policy) – визначає вимоги щодо регулярного резервного копіювання інформації.

3.3.4 Організації моніторингу, аудиту та політик безпеки

Для максимально ефективного забезпечення безпеки інформації в хмарних середовищах рекомендується дотримуватись таких практик:

Впровадження централізованого моніторингу всіх подій безпеки з використанням SIEM-рішень.

Регулярне проведення аудитів безпеки та penetration testing для своєчасного виявлення вразливостей.

Постійний перегляд і актуалізація політик безпеки, особливо після впровадження нових сервісів чи технологій.

Навчання персоналу щодо вимог безпеки та відповідальності за дотримання політик.

На рисунку 3.3 можна побачити схематично, як саме відбувається моніторинг в хмарі

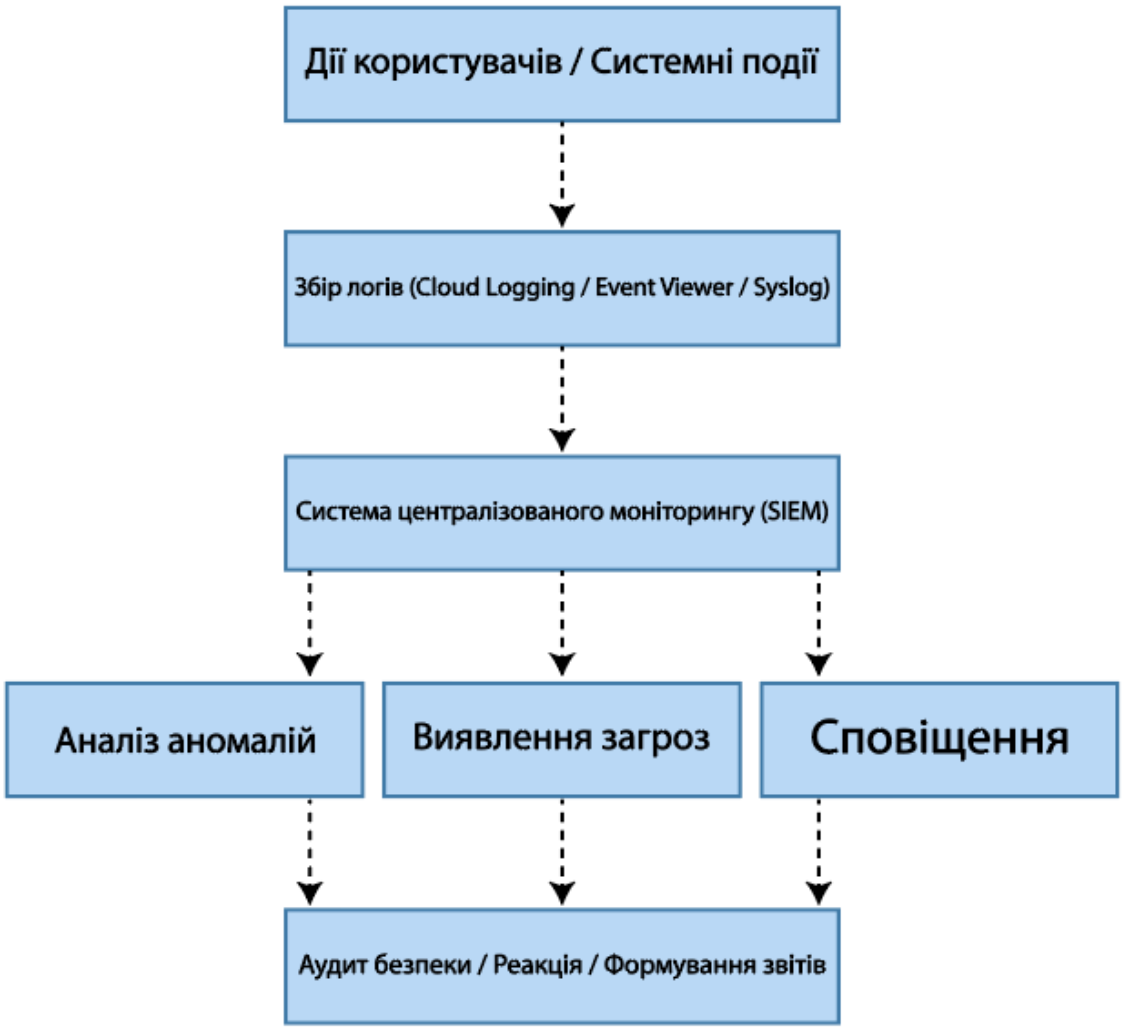

Рисунок 3.3 – Схема моніторингу та аудиту безпеки в хмарі

Отже, моніторинг, аудит і політики безпеки становлять фундаментальні складові захисту інформації в хмарних середовищах. Ефективний моніторинг забезпечує швидке виявлення та реагування на інциденти, регулярні аудити контролюють дотримання стандартів безпеки, а чітко сформульовані політики встановлюють правила безпечної роботи персоналу та IT-інфраструктури. Комплексне застосування цих заходів гарантує високий рівень захисту даних і надійність хмарних сервісів компанії.

4 ПРАКТИЧНА ЧАСТИНА — ДОСЛІДЖЕННЯ БЕЗПЕКИ ЕЛЕКТРОННОЇ ПОШТИ

4.1 Загальний опис сервісу Gmail та його функцій безпеки

Gmail — це безкоштовний хмарний поштовий сервіс від компанії Google, який забезпечує користувачам зручний інтерфейс для надсилання та отримання електронних листів, зберігання файлів і інтеграцію з іншими продуктами Google. Завдяки тісній взаємодії з Google Drive, Google Workspace, Google Meet та іншими сервісами, Gmail виконує роль не лише поштового клієнта, а й частини комплексної платформи для спілкування, співпраці та управління цифровими ресурсами.

Сервіс Gmail широко використовується як приватними користувачами, так і організаціями по всьому світу, що висуває підвищені вимоги до захисту даних. Він забезпечує доступ з будь-яких пристроїв через веб-браузер або мобільні додатки, підтримує обмін великими обсягами інформації та вкладень, що робить його зручним і надійним інструментом для щоденної роботи.

Окрім зручності, Gmail також забезпечує високий рівень інформаційної безпеки, використовуючи як власні технології, так і стандарти галузі, що можна побачити на рисунку 4.1. Його механізми захисту базуються на багаторівневому підході, який охоплює:

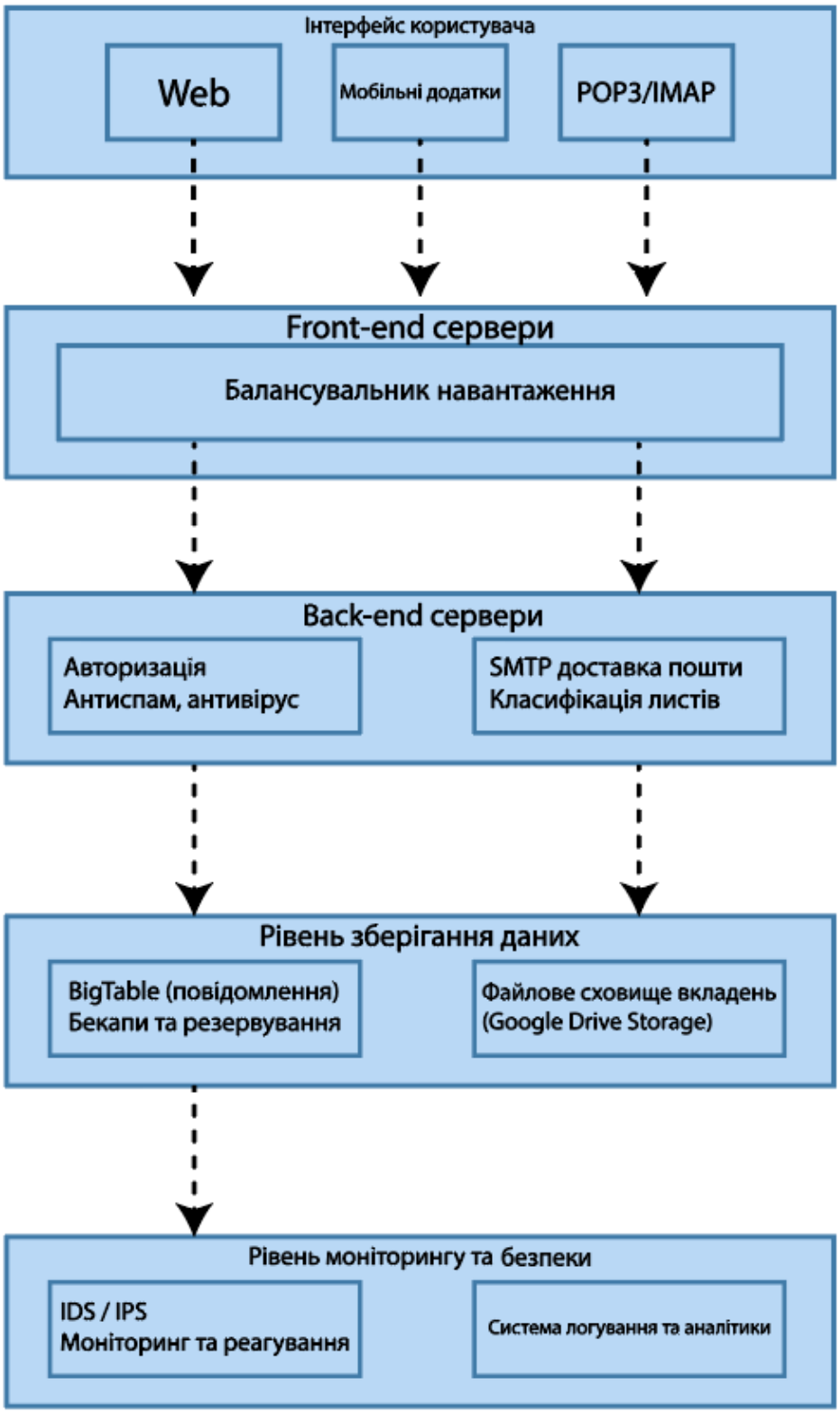

Рисунок 4.1 - Схема архітектури сервісу Gmail

Фільтрацію спаму та фішингових повідомлень

Gmail автоматично розпізнає та переміщує небажані листи у папку «Спам». У разі виявлення фішингового вмісту або підозрілих посилань користувач отримує попередження. Такі повідомлення можуть містити ознаки шахрайства, спроби викрасти облікові дані або шкідливі вкладення.

Сканування вкладень на наявність вірусів та шкідливого ПЗ

Усі вкладення в Gmail проходять миттєву перевірку на наявність шкідливого коду або небезпечних форматів. Зокрема, сервіс блокує надсилання виконуваних файлів із розширеннями .exe, .js, .bat та іншими, щоб запобігти розповсюдженню вірусів і троянських програм. Якщо користувач намагається відправити такий файл, він отримує повідомлення про блокування вкладення з огляду на безпеку.

Шифрування листування

Усі повідомлення в Gmail шифруються за допомогою протоколу TLS (Transport Layer Security), що забезпечує захист даних під час передачі між клієнтами та серверами. Це запобігає можливості перехоплення вмісту листів під час їх маршрутизації в мережі Інтернет.

Підтримка двофакторної автентифікації (2FA):

Gmail підтримує багатофакторну автентифікацію, яка, крім пароля, вимагає додаткового підтвердження через SMS, додаток Google Authenticator або фізичний ключ безпеки. Такий підхід суттєво знижує ризик компрометації акаунта навіть у випадку викрадення пароля.

Аналіз поведінки користувача

Система безпеки Gmail відстежує аномальну активність у акаунті, таку як вхід із незнайомої IP-адреси, спроби доступу з підозрілих регіонів або надсилання великої кількості листів за короткий проміжок часу. У разі виявлення таких подій Google може тимчасово обмежити доступ до акаунта.

Інтегрована панель безпеки акаунта (Google Account Security)

Користувач має можливість у будь-який час переглянути список пристроїв, з яких відбувався вхід до акаунта, увімкнути додаткові засоби захисту, змінити пароль або обмежити доступ стороннім застосункам. Крім того, Google регулярно рекомендує проходити «Перевірку безпеки акаунта», яка допомагає оцінити та покращити налаштування безпеки.

Gmail виконує не лише роль електронної пошти, а й є комплексною хмарною платформою з високим рівнем захисту, що постійно оновлюється відповідно до нових кіберзагроз. Саме тому цей сервіс є зручним об’єктом для вивчення механізмів інформаційної безпеки в хмарних обчисленнях і добре підходить для навчального аналізу сучасних методів захисту даних.

4.2 Моделювання фішингової атаки та реакція Gmail

Фішинг — один із найпоширеніших методів соціальної інженерії, що використовується зловмисниками для викрадення облікових даних, встановлення шкідливого програмного забезпечення або несанкціонованого доступу до конфіденційної інформації. Gmail, як один із провідних поштових сервісів у світі, часто стає об’єктом фішингових атак. Тому платформа впроваджує багаторівневий захист для протидії таким загрозам.

У ході дослідження було змодельовано типовий сценарій фішингової атаки. Створено електронний лист, що імітував офіційне повідомлення від ділового партнера. Деталі схеми наведено на рисунку 4.2. Тема листа — «Терміновий запит клієнта» — мала спонукати користувача до швидкої реакції. До листа було додано файл під назвою zapyt_clienta.exe, що виглядав як службовий документ, але містив примітивний кейлогер — програму для запису натискань клавіш.

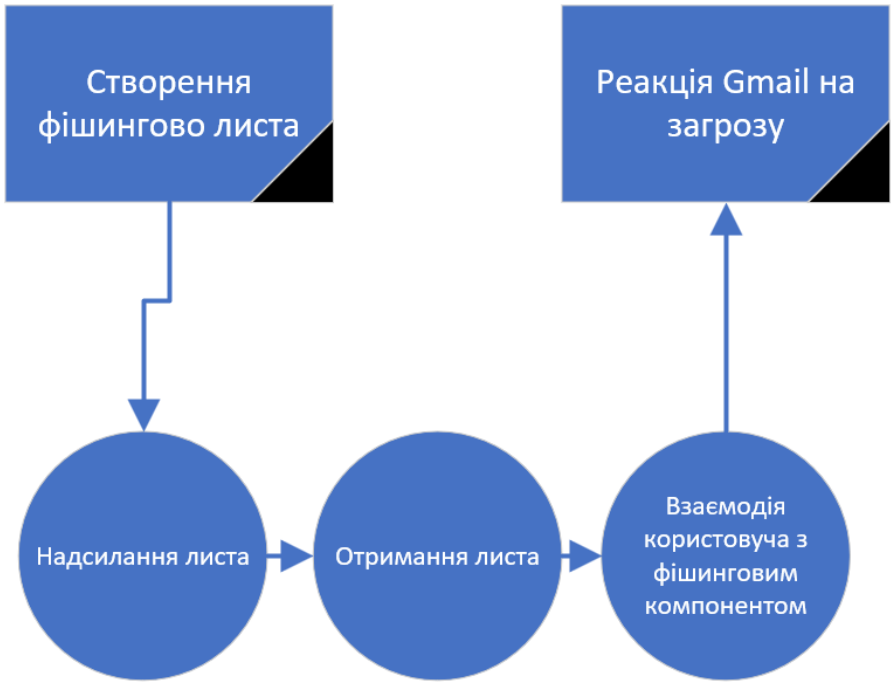

Рисунок 4.2 - Схема моделювання фішингової атаки на Gmail

Система безпеки Gmail миттєво спрацювала — при спробі надіслати листа з таким вкладенням, з’явилося попередження:

«Вкладення було заблоковано з міркувань безпеки. Gmail не дозволяє надсилати виконувані файли, які можуть містити віруси або інші шкідливі програми».

Цей механізм працює на основі кількох рівнів перевірки:

Аналіз розширення файлу: Gmail автоматично блокує розширення .exe, .bat, .cmd, .js та інші, які мають високий ризик.

Сканування сигнатур: порівняння вмісту вкладення з базою відомих зразків шкідливого ПЗ.

Контекстна перевірка листа: враховується не лише вміст, а й шаблон поведінки (тема, кількість одержувачів, IP-адреса, країна відправника).

Приклад фішингового листа:

Від: support.google.services.verify@gmail.com

Тема: Ваш обліковий запис буде видалено через 24 години

Текст: Ми виявили підозрілу активність. Для уникнення втрати доступу, підтвердьте ваш акаунт за посиланням:

https://google-verify-user-check.com/login

Gmail класифікує такі листи як потенційно небезпечні через такі ознаки:

Виконуване розширення у вкладеннях

Відсутність цифрового підпису або сертифіката видавця

Посилання на зовнішні ресурси, які імітують реальні сервіси Google

Вміст листа з терміновим закликом до дії

Крім блокування небезпечних вкладень, Gmail також може позначати подібні повідомлення жовтим банером зверху листа з текстом: "Це повідомлення може бути фішинговим. Не натискайте посилання і не надавайте свої особисті дані."

Отриманий результат, що демонструє блокування вкладення, підтверджує ефективність механізмів виявлення загроз у Gmail. Така поведінка є прикладом проактивного підходу до захисту користувача та підвищує загальний рівень довіри до сервісу.

Успішний фішинг — приклад потенційної загрози

Незважаючи на наявність потужних засобів захисту, жодна система не є на 100% захищеною. Успішний фішинг може мати місце тоді, коли користувач:

Ігнорує попередження Gmail

Відкриває посилання з фальшивого листа

Вводить свої облікові дані на підробленому сайті

Приклад:

Користувач отримав лист із темою: "Google: Підтвердження платежу"

Відправник: billing-support@googlesecure.com (маскування під офіційного)

У листі: "Ваша підписка буде автоматично поновлена. Для скасування перейдіть за посиланням."

Посилання веде на сайт google-billing.com (латинська "e" замінена на кириличну)

Користувач натискає посилання, потрапляє на сайт-клон Gmail, вводить свій email та пароль — і дані миттєво передаються зловмиснику.

Такі випадки демонструють, що навіть з високим рівнем автоматичного захисту, людський фактор залишається головною вразливістю. Тому навчання користувачів кібергігієні є важливою частиною загальної політики безпеки.

Крім блокування небезпечних вкладень, Gmail також може позначати подібні повідомлення жовтим банером зверху листа з текстом: "Це повідомлення може бути фішинговим. Не натискайте посилання і не надавайте свої особисті дані."

Результат демонструє блокування вкладення, підтверджує ефективність механізмів виявлення загроз у Gmail. Така поведінка є прикладом проактивного підходу до захисту користувача та підвищує загальний рівень довіри до сервісу.

Для моделювання потенційної загрози було також створено умовний файл із кодом, що імітує кейлогер, як показано на рисунку 4.3.

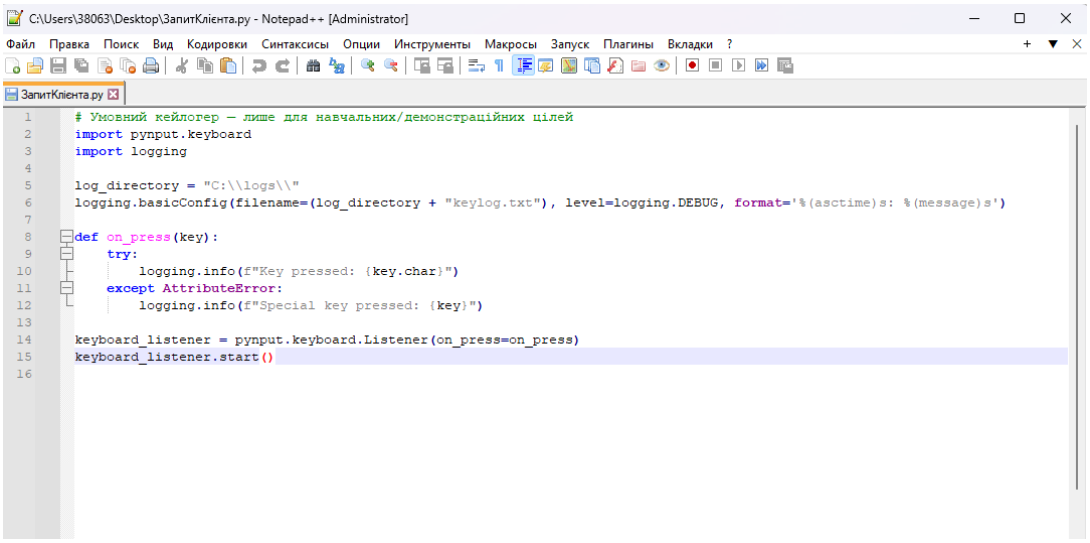

Рисунок 4.3 - Процес створення Python-скрипту з функціоналом кейлогера

Цей скрипт зчитує натискання клавіш та записує їх у текстовий файл. Після створення .py-файлу він був перетворений у виконуваний .exe за допомогою інструменту PyInstaller. Далі файл було протестовано через завантаження у Google Drive та спробу надіслати через Gmail. На рисунку 4.4 видно, що Google Drive, дав змогу завантажити вірусний файл на свій портал, але при завантаженні попереджую користувача про можливий вірус.

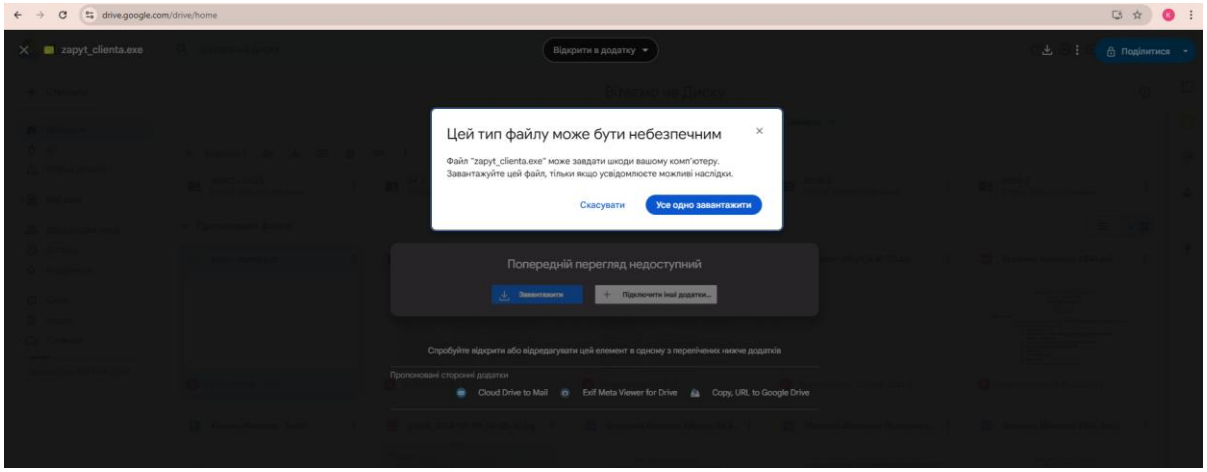

Рисунок 4.4 - Завантаження .exe у Google Диск — файл приймається без повідомлень, але при завантаженні попередження про небезпеку

Gmail навіть не дав змоги відправити умовний фішинговий лист, що видно на рисунку 4.5

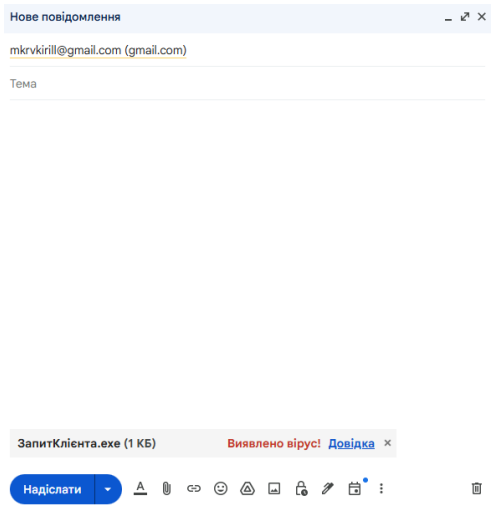

Рисунок 4.5 - Спроба надсилання .exe-файлу через Gmail — файл автоматично блокується системою безпеки з повідомленням "Заблоковано з міркувань безпеки"

Цей приклад ілюструє, як Gmail запобігає поширенню потенційно шкідливого програмного забезпечення, навіть якщо воно маскується під звичайний вкладений файл. Це підтверджує важливість вбудованих механізмів безпеки в хмарних сервісах та їх здатність проактивно виявляти загрози ще до взаємодії користувача з повідомленням. Такий підхід підвищує рівень захисту і сприяє зростанню довіри до платформи.

1) Аналіз розширення файлу

Gmail автоматично блокує файли з розширеннями, які часто використовуються для доставки шкідливого ПЗ. До них належать:

.exe, .bat, .cmd, .scr, .pif — класичні виконувані файли

.js, .vbs, .jse, .wsf — скрипти, які можуть виконувати дії без згоди користувача

.jar — архіви Java-програм, що також можуть містити шкідливий код

.msi — інсталятори

.com, .cpl, .gadget — спеціалізовані виконувані формати

Тригери: наявність одного з цих розширень у вкладенні автоматично викликає блокування.

2) Сканування вмісту файлу

Gmail не обмежується перевіркою лише розширення — навіть файли у форматі .zip, .rar, .7z розпаковуються та аналізуються на сервері:

якщо всередині архіву є .exe або .js, лист буде заблоковано

якщо вміст архіву містить текстові патерни (див. нижче), він теж може бути заблокований

3) Аналіз сигнатур і хешів

Gmail має доступ до бази відомих вірусів, троянів і кейлогерів. Перед надсиланням файл перевіряється на відповідність цим сигнатурам (аналогічно антивірусам).

Якщо файл співпадає по SHA256 або MD5 з відомим зразком — блокується негайно.

4) Контентна фільтрація (тригери в коді)

Файли, що містять ключові слова, можуть бути помічені як підозрілі — навіть якщо мають «безпечне» розширення.

Приклади тригерних слів і патернів у коді:

keyboard.read_event, GetAsyncKeyState, logging.info(key)

os.system('shutdown'), subprocess, winreg

write("password=", grab_credentials, clipboard, inject, payload

вказані шляхи: C:\\Users\\, AppData\\Roaming\\, keylog.txt

рядки типу: with open(..., \"a\") as f, socket.send, ftp.put

5) Аналіз поведінки скрипта (sandbox-аналіз)

Gmail може тимчасово запустити вкладення в ізольованому середовищі (sandbox) і перевірити:

чи створює файл підключення до інтернету

чи намагається записати дані у системні папки

чи змінює реєстр Windows (winreg)

чи збирає натискання клавіш

6) Аналіз метаданих та сертифікатів

Відсутність цифрового підпису, дивне ім’я файлу (invoice_urgent_4422.exe), велика кількість нестандартних символів — усе це викликає підозру.

Gmail виявляє небезпечне вкладення ще до надсилання листа, перевіряючи не лише розширення, але й вміст, сигнатури, код, поведінку та навіть архіви всередині вкладень.

Це робить сервіс одним з найефективніших у боротьбі з поширенням шкідливого ПЗ через електронну пошту.

4.3 Багатофакторної автентифікації в хмарному середовищі Gmail

Для підвищення безпеки хмарних облікових записів особливу увагу приділяють впровадженню багатофакторної автентифікації (Multi-Factor Authentication, MFA), яка суттєво ускладнює несанкціонований доступ до ресурсів. У рамках практичного дослідження було проаналізовано механізми двофакторної автентифікації (2FA), реалізовані у поштовому сервісі Gmail, а також змодельовано сценарій активації захисту облікового запису з демонстрацією взаємодії користувача із системою.

Архітектурні особливості 2FA

Сучасна реалізація 2FA базується на розподіленій перевірці, коли для доступу до облікового запису необхідно пройти дві незалежні перевірки автентичності:

Щось, що користувач знає — пароль, PIN-код

Щось, що користувач має — мобільний пристрій, токен, біометричний ключ

Gmail підтримує наступні типи другого фактору:

Одноразові паролі (OTP), надіслані через SMS або дзвінок

Мобільні підтвердження Google Prompt

Генератори кодів (TOTP) — Google Authenticator, Authy

Апаратні ключі (FIDO2/U2F)

Резервні коди (офлайн-доступ)

Сценарій активації 2FA в Gmail

Процес включення механізму автентифікації складається з наступних кроків:

Перехід до консолі безпеки акаунта → розділ «Вхід у акаунт Google»

Активація «Двоетапної перевірки» з підтвердженням пароля

Вибір одного або декількох факторів

Генерація резервних кодів для аварійного відновлення доступу

Моделювання логіки двофакторної автентифікації (умовний приклад)

Для ілюстрації внутрішньої логіки взаємодії між сервісом та користувачем на рівні авторизації наведу приклад псевдокоду на рисунку 4.6

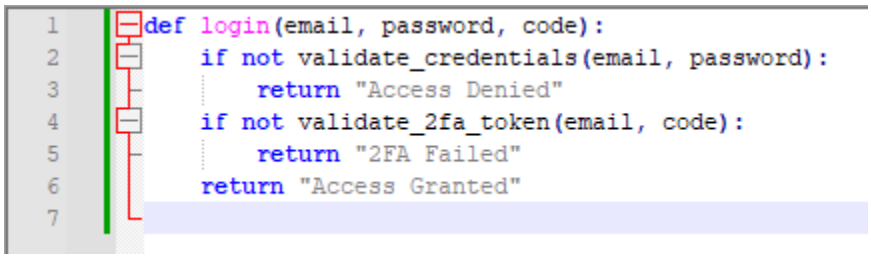

Рисунок 4.6 – Псевдокод внутрішньої логіки взаємодії між сервісом та користувачем

Така логіка підтверджує, що доступ надається лише за умови успішного проходження обох етапів: перевірки пароля та другого фактору.

Механізми 2FA, реалізовані у Gmail, відповідають найкращим практикам галузі з точки зору безпечного управління автентифікацією. Активація двофакторної

перевірки значно знижує ризики фішингу, атаки методом перебору, компрометації сесій або застосування шкідливого ПЗ на кшталт кейлогерів.

Імплементація 2FA є обов'язковою складовою формування ефективного політики кіберзахисту в умовах використання хмарних обчислювальних технологій.

4.4 Системи журналювання та моніторингу доступу в хмарному середовищі Gmail: аналіз, можливості, практичне застосування

Одним із ключових елементів забезпечення безпеки хмарних сервісів є впровадження системи журналювання подій (audit trail) та інструментів безперервного моніторингу доступу до акаунтів. У випадку Gmail ця функціональність реалізована через централізований модуль сповіщень про активність облікового запису та історію входів, що надає користувачу прозорий контроль над діями в межах його акаунта.

Архітектура моніторингу доступу в Gmail

У рамках сервісу Google Account кожен користувач має доступ до розділу «Ваші пристрої» (Your Devices), що відображає історію входів до акаунта з наступними параметрами:

Назва пристрою (тип операційної системи, браузера або мобільного застосунку)

Географічне положення (визначене за IP-адресою)

Час останнього доступу

Метод входу (браузер, застосунок, API)

Ці параметри формують деталізовану картину доступу, дозволяючи своєчасно виявляти аномальні або несанкціоновані входи.

Критерії виявлення підозрілої активності

Алгоритми Google автоматично ідентифікують потенційно небезпечну активність за такими ознаками:

Спроба входу з нового географічного регіону

Вхід з невідомого пристрою

Активація підозрілих API-з’єднань

Нетипова активність у нічний час або з скомпрометованих IP-адрес

У разі виявлення такої активності користувачу надсилається миттєве push-сповіщення, а також відповідне повідомлення на зареєстровану електронну пошту.

Механізм реагування

Інтерфейс Google Account надає можливість оперативного реагування:

Вихід із акаунта на підозрілих пристроях

Зміна пароля

Увімкнення 2FA (якщо не активовано)

Відкликання дозволів для сторонніх застосунків

Таким чином, користувач має повноцінний інструментарій для самостійного забезпечення оперативного контролю за безпекою акаунта.

Приклад сценарію реагування

У результаті перевірки було виявлено вхід до акаунта з IP-адреси, яка географічно не відповідає поточному місцезнаходженню користувача. Gmail автоматично ініціював сповіщення про спробу входу та запропонував пройти перевірку безпеки. Користувач здійснив вихід із усіх пристроїв, змінив пароль та увімкнув двофакторну автентифікацію.

Функції журналювання активності та відображення підключених сесій у Gmail є важливими складовими превентивного захисту користувача. Вони підвищують прозорість взаємодії з хмарним сервісом і підтримують принцип Zero Trust, за яким кожна дія потребує підтвердження та перевірки довіри.

4.5 Політика керування сторонніми доступами до хмарного акаунта: контроль, ризики та практичні механізми реалізації у Gmail

В контексті хмарної безпеки одним із ключових ризиків потенційного витоку даних є автоматизований або фоновий доступ сторонніх застосунків до акаунта користувача. Gmail, як частина екосистеми Google, підтримує інтеграцію з численними зовнішніми сервісами та додатками, що потребує суворого контролю над наданими дозволами для запобігання небажаному доступу.

Архітектура авторизації через OAuth 2.0

Google впроваджує механізм авторизації доступу до користувацьких даних за допомогою протоколу OAuth 2.0, що дозволяє стороннім додаткам отримувати обмежені права без розкриття основного пароля. Незважаючи на стандартизовану модель доступу, підвищені ризики виникають, коли користувач надає надмірні або непомітні дозволи, не усвідомлюючи можливих наслідків.

Потенційні ризики доступу сторонніх застосунків:

Читання або надсилання пошти від імені користувача

Доступ до Google Drive та контактів

Моніторинг календаря або геолокаційної інформації

Збір метаданих без прямого втручання у вміст

У разі компрометації стороннього сервісу, такого як поштові клієнти чи додатки для підвищення продуктивності, зловмисники можуть скористатися наданими дозволами для доступу до Gmail без необхідності зламу самого облікового запису.

У межах практичної частини було здійснено аналіз активних з’єднань з обліковим записом Google. У панелі “Керування доступом сторонніх застосунків” було виявлено декілька сервісів із широкими повноваженнями (наприклад, «читання та надсилання листів», «керування файлами в Drive»).

Після аналізу рівня доступу здійснено ручне відкликання надлишкових дозволів, що не використовувалися протягом тривалого часу, приклад наведено на рисунку 4.7

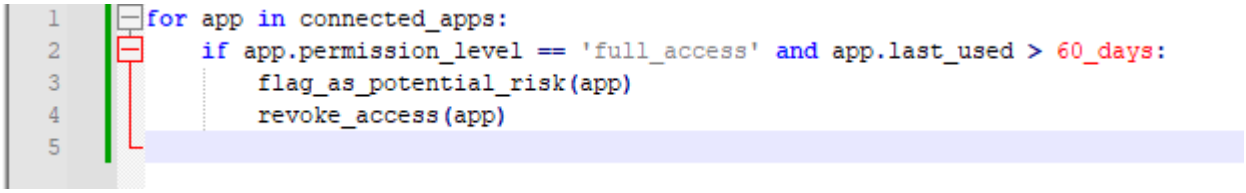

Рисунок 4.7 - Умовна логіка оцінки ризику (псевдокод)

Цей умовний фрагмент демонструє базову стратегію виявлення додатків із завищеними повноваженнями, які неактивні протягом визначеного періоду.

Ефективне управління доступами сторонніх додатків є важливою складовою інформаційної гігієни користувача в хмарному середовищі. Інструменти Google для контролю дозволів дають змогу користувачам легко впливати на безпеку свого облікового запису без необхідності володіти глибокими технічними знаннями. Регулярна перевірка активних авторизацій стає особливо актуальною на фоні стрімкого зростання кількості інтеграцій та хмарних сервісів.

У рамках практичного дослідження проведено всебічний аналіз механізмів безпеки, реалізованих у хмарному сервісі Gmail, з особливим акцентом на виявлення фішингових загроз, управління автентифікацією та контроль доступу. Моделювання сценаріїв атак і реакцій системи підтвердило, що Gmail використовує багаторівневу архітектуру захисту, яка забезпечує як проактивне виявлення шкідливої активності, так і дає користувачеві можливість активно контролювати безпеку власного акаунта.

4.5 Моделювання загроз у середовищі AWS

У межах практичної частини дослідження було змодельовано потенційний інцидент безпеки у хмарному середовищі Amazon Web Services (AWS), аналогічно до попереднього кейсу з Gmail.

Було створено хмарне сховище Amazon S3 (bucket з назвою test-bucket12121211fwefew), у якому було розміщено умовний шкідливий файл — zapyt_clienta.exe, що імітує виконуваний файл кейлогера. Його завантаження відбулося успішно без жодних попереджень або обмежень з боку платформи AWS.

Наступним кроком було надання публічного доступу до об’єкта. Спочатку була відключена система Block Public Access, що за замовчуванням забороняє загальнодоступний доступ до будь-яких об'єктів у S3. Потім була створена Bucket Policy, яка дозволяє будь-якому користувачу Інтернету завантажити файли з цього bucket.

Після застосування політики пряме посилання на файл zapyt_clienta.exe стало активним:
https://test-bucket12121211fwefew.s3.eu-north-1.amazonaws.com/zapyt_clienta.exe\
AWS не виконала жодної перевірки вмісту файлу на шкідливість. Об'єкт був розміщений і доступний для завантаження без втручання захисних механізмів платформи, як зображено на рисунку 4.8. Проте, при спробі завантажити файл через браузер Google Chrome, отримав повідомлення: "Підозріле завантаження заблоковано", наведено скриншот на рисунку 4.9. Це вказує на те, що механізми безпеки AWS зосереджені переважно на контролі доступу (через ACL, Bucket Policy, IAM), але не включають вбудований антивірусний аналіз або фільтрацію шкідливого коду. Виявлення потенційної загрози було здійснене лише на рівні браузера, а не самої хмарної платформи.

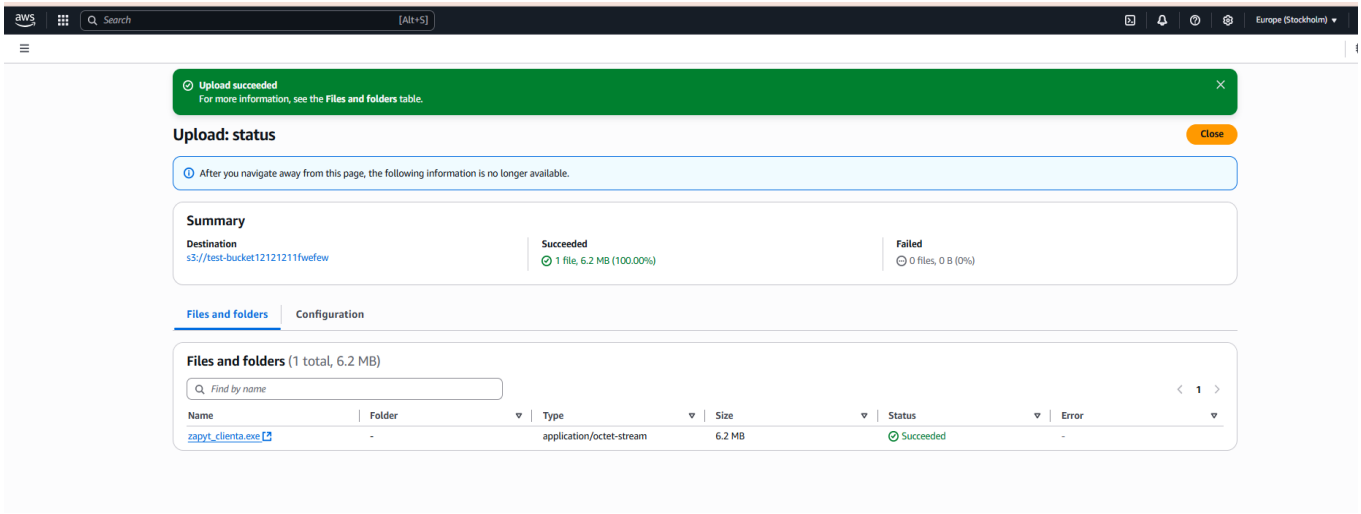

Рисунок 4.8 – Успішне завантаження файлу на AWS

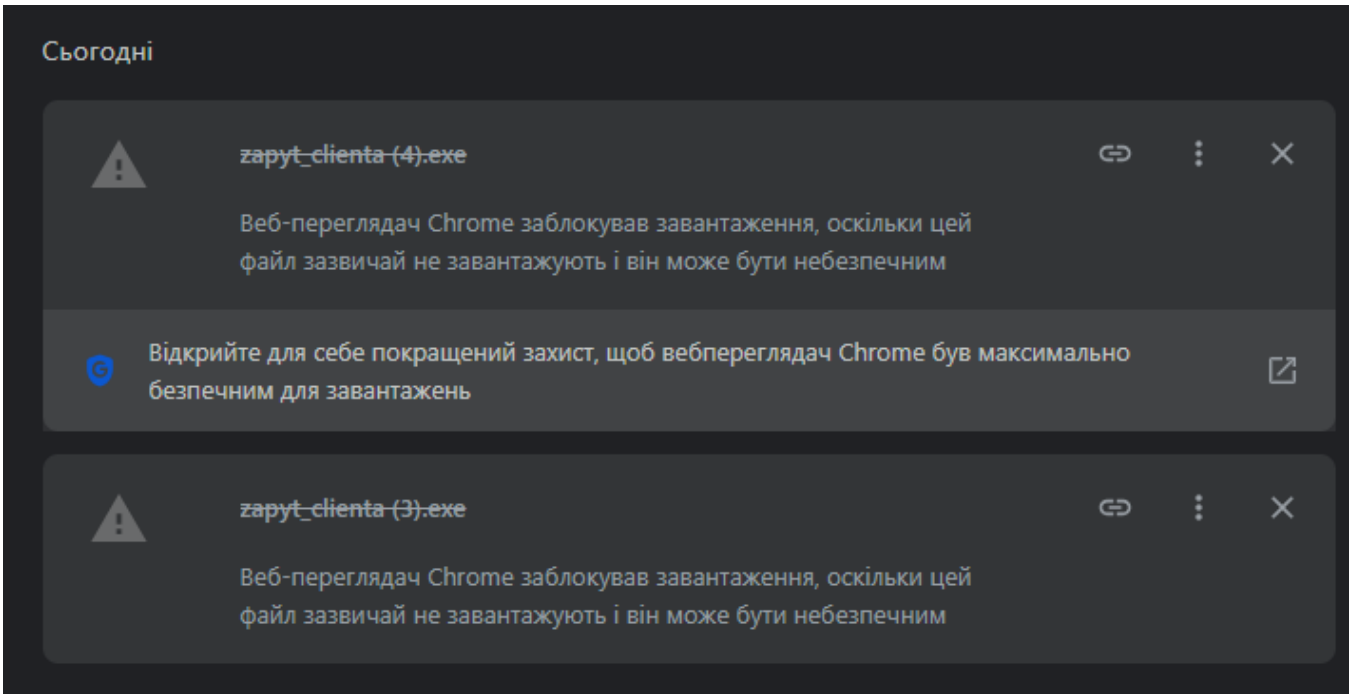

Рисунок 4.9 – Підозріле завантаження заблоковано

ВИСНОВКИ

У рамках виконання дипломної роботи на тему «Захист інформації в хмарних обчисленнях» проведено всебічне дослідження теоретичних, аналітичних, методологічних та практичних аспектів інформаційної безпеки в хмарних середовищах. Отримані результати дають змогу сформулювати низку ключових висновків і рекомендацій для підвищення рівня кіберзахисту під час застосування хмарних технологій.

1) Теоретичне обґрунтування поняття хмарних обчислень

У першому розділі проведено детальний аналіз сутності, архітектури та класифікації хмарних обчислень. Визначено, що хмарні обчислення є ключовим елементом сучасної цифрової інфраструктури, який надає доступ до обчислювальних ресурсів через Інтернет у форматі сервісу. Описано основні моделі надання послуг (IaaS, PaaS, SaaS) та моделі розгортання (публічна, приватна, гібридна, мультихмара), а також розглянуто спеціалізовані сервіси для вирішення вузькоспеціалізованих задач (DaaS, BaaS, FaaS).

Аналіз показав, що ефективне впровадження хмарних рішень вимагає не лише технічної компетентності, а й усвідомлення ризиків, пов’язаних із передачею контролю над інфраструктурою стороннім провайдерам. Отже, питання безпеки повинні бути невід’ємною частиною кожного етапу життєвого циклу хмарного сервісу.

2) Аналіз загроз та вразливостей у хмарних середовищах

У другому розділі систематизовано основні загрози інформаційній безпеці, що виникають у процесі використання хмарних обчислень. До найважливіших ризиків віднесено: несанкціонований доступ, витік або втрату даних, атаки типу «відмова в обслуговуванні» (DDoS), уразливості API та віртуалізаційного шару, внутрішні

загрози, помилки конфігурації (misconfiguration) та проблеми багатокористувацької ізоляції.

Виділено типовий набір вразливостей, притаманних хмарним сервісам, а також проведено огляд методів моделювання загроз (STRIDE, DREAD, OCTAVE, дерева атак) та підходів до оцінювання ризиків. Аналіз цих даних дозволив зробити висновок, що ефективний захист у хмарних середовищах неможливий без формалізованого ризик-менеджменту, який поєднує кількісні та якісні методи оцінки.

3) Методи та засоби захисту інформації

Третій розділ був присвячений аналізу сучасних технологій захисту інформації в хмарних середовищах. Серед ключових підходів розглянуто криптографічні алгоритми (AES, RSA, ECC, TLS), цифрові підписи, хеш-функції, багатофакторну автентифікацію (2FA/MFA), системи виявлення вторгнень (IDS/IPS), політики контролю доступу (RBAC, ABAC), аудит журналів доступу та логування подій, а також резервне копіювання і планування аварійного відновлення (DR/BCP).

У результаті дослідження встановлено, що використання окремих технічних засобів не забезпечує належного рівня безпеки. Надійний захист досягається лише за умови впровадження комплексного підходу, що об’єднує технологічні, організаційні та управлінські заходи.

4) Практичне дослідження безпекових механізмів на прикладі Gmail

У четвертому розділі наведено моделювання типових сценаріїв атак та відповідних механізмів реагування у реальному хмарному середовищі на прикладі сервісу Gmail. Розглянуто реакцію системи на виявлення фішингових вкладень, блокування спроб завантаження шкідливих файлів (наприклад, кейлогера), ефективність двофакторної автентифікації, можливості моніторингу активності входів, а також контроль і відкликання доступу сторонніх додатків.

Моделювання показало, що внутрішні механізми безпеки Gmail працюють дуже ефективно, застосовуючи багаторівневу перевірку — від аналізу сигнатур до sandbox-тестування. Водночас стало зрозуміло, що роль користувача в підтримці безпеки не менш важлива: активне використання двофакторної автентифікації, регулярна перевірка доступів і пильність щодо підозрілої активності — ключові складові захисту.

5) Узагальнюючі висновки

Проведене дослідження дозволило сформувати комплексне уявлення про специфіку захисту інформації в хмарних середовищах. Серед ключових висновків варто виділити:

Хмарні обчислення — це технологія, що забезпечує потужні можливості, але водночас створює нові вектори атак.

Захист інформації у хмарі вимагає постійного моніторингу загроз, оновлення інструментів безпеки, а також дотримання принципів Zero Trust.

Вкрай важливо усвідомлювати модель спільної відповідальності: користувач відповідає за налаштування, контроль доступу та автентифікацію, тоді як провайдер забезпечує фізичну безпеку, мережеву інфраструктуру та базову платформу.

Ефективний захист можливий лише при поєднанні технічних, нормативних і організаційних заходів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мелл, П., Ґранс, Т. (2011). Визначення хмарних обчислень за NIST (NIST Special Publication 800-145). Гейтерсбург, Меріленд.
2. Ґранс, Т., Янсен, В. (2011). Рекомендації щодо безпеки та конфіденційності в публічному хмарному середовищі (NIST Special Publication 800-144). Гейтерсбург, Меріленд.
3. ISO/IEC 17788:2014. Інформаційні технології – Хмарні обчислення – Огляд і словник. Женева: ISO, 2014.
4. ISO/IEC 27017:2015. Інформаційні технології – Техніки безпеки – Рекомендації щодо контролю безпеки інформації для хмарних послуг. Женева: ISO, 2015.
5. ISO/IEC 27018:2019. Інформаційні технології – Техніки безпеки – Рекомендації щодо захисту персональних даних у публічних хмарах. Женева: ISO, 2019.
6. Самі, Р., Хонан, Б., Рівайс, Дж. (2014). Посібник CSA з хмарних обчислень: Реалізація конфіденційності та безпеки. Syngress/Elsevier.
7. Cloud Security Alliance (2019). ТОП-Загрози хмарним обчисленням: Відомі одинадцять. Cloud Security Alliance.
8. ENISA (Агенція з кібербезпеки ЄС). (2009). Хмарні обчислення: Переваги, ризики та рекомендації щодо інформаційної безпеки. Звіт ENISA..
9. OWASP (2022). Шпаргалка з безпечної архітектури хмари. OWASP Cheat Sheet Series.
10. Amazon Web Services (2020). Архітектурні принципи AWS (AWS Well-Architected Framework). Сіетл, Вашингтон.
11. Microsoft (2022). Орієнтовані на безпеку стандарти Microsoft Cloud Security Benchmark. Редмонд, Вашингтон.
12. Parast, F. K., Yekta, K. I., Kent, B., & Hakak, S. (2022). Безпека в хмарних обчисленнях: Огляд моделей сервісів. Computers & Security, 114, 102580.

13. Кулаковська, І. (2024). Ризики використання хмарних технологій. Вісник Хмельницького національного університету, № 5(341), 45–52.
14. Акбарова, М. Р. (2022). Безопасность и защита данных в облачных технологиях. Universum: Технические науки, 10–1(103), 17–19.
15. Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Безпека в хмарних обчисленнях: Можливості та виклики. Information Sciences, 305, 357–383.
16. Hashizume, K., Rosado, D. G., Fernandez-Medina, E., & Fernandez, E. B. (2013). Аналіз проблем безпеки для хмарних обчислень. Journal of Internet Services and Applications, 4(1), 5.
17. Dropbox Security Whitepaper. – Режим доступу: https://www.dropbox.com/security. Дата звернення: 14.03.2025.
18. ISO/IEC 27001:2022. Системи управління інформаційною безпекою – Вимоги. Женева: ISO, 2022.
19. Gmail Help. Check devices & account activity – Режим доступу: https://support.google.com/mail/answer/45938. Дата звернення: 12.03.2025.