DOI 10.31891/2307-5732-2024-341-5-6
УДК 004.891: 004.9

КУЛАКОВСЬКА ІНЕССА
Чорноморський національний університет імені Петра Могили, м. Миколаїв
https://orcid.org/0000-0002-8432-1850
e-mail: inessa.kulakovska@chmnu.edu.ua

# РИЗИКИ ВИКОРИСТАННЯ ХМАРНИХ ТЕХНОЛОГІЙ

*Хмарні технології стали невід'ємною частиною сучасного цифрового світу, пропонуючи багато переваг для бізнесу та приватних користувачів. Їхня гнучкість, масштабованість та економічна вигода роблять їх привабливим вибором для зберігання даних, розробки програмного забезпечення та надання інших IT-послуг. Однак, поряд з перевагами, хмарні технології несуть у собі й певні ризики, які не можна ігнорувати. Дослідження цих ризиків є надзвичайно актуальним.*

*Хмарні технології надають послуги на вимогу через Інтернет за допомогою великого обсягу віртуального сховища. Основними особливостями хмарних рішень є те, що користувач не виконує налаштування обчислювальної інфраструктури, а вартість послуг нижча. Останніми роками хмарні обчислення інтегруються з індустрією та багатьма іншими сферами, що заохочує досліджувати нові суміжні технології та ШІ. Завдяки доступності хмарних послуг і масштабованості для обчислювальних процесів окремі користувачі та організації передають свої програми, дані та послуги на сервер хмарного сховища. Незважаючи на свої переваги, трансформація локальних обчислень у віддалені обчислення принесла багато питань безпеки та проблем як для споживача, так і для постачальника. Багато хмарних сервісів надаються третьою стороною, що створює нові загрози безпеці. Хмарний провайдер надає свої послуги через Інтернет і використовує багато вебтехнологій, що створює і тут проблеми безпеки. У дослідженні розглядаються основні особливості хмарних технологій, проблеми безпеки, потенційні загрози та їх вирішення. Описано шість ключових тем, пов'язаних із безпекою хмари, структуру хмарної архітектури, моделі обслуговування та розгортання, хмарні технології, концепції безпеки хмари, загрози та атаки. У статті також обговорюється багато відкритих дослідницьких питань, пов'язаних із методами оцінки ризиків до кожної з вразливостей використання хмари.*

*Залежність від хмарних сервісів постійно зростає, адже все більше компаній та організацій переходять на їх використання. Це робить їх більш вразливими до збоїв, кібератак та інших проблем, які можуть призвести до значних втрат даних, фінансових збитків та репутаційних втрат.*

*Ключові слова: хмарні послуги, вразливості хмарних сервісів, оцінка ризиків використання хмарних технологій, методи оцінки ризиків.*

KULAKOVSKA INESSA
Petro Mohyla Black Sea National University, Mykolayiv, UA

## OVERVIEW OF THE STATUS AND TRENDS OF RESEARCH ON THE RISKS OF THE USE OF CLOUD TECHNOLOGIES

*Cloud technologies have become an integral part of today's digital world, offering many advantages for businesses and private users. Their flexibility, scalability, and cost-effectiveness make them an attractive choice for data storage, software development, and other IT services. However, along with the advantages, cloud technologies also carry certain risks that cannot be ignored. The study of these risks is extremely urgent.*

*Cloud technology provides on-demand services over the Internet using a large amount of virtual storage. The main features of cloud solutions are that the user does not configure the computing infrastructure, and the cost of services is lower. In recent years, cloud computing has been integrated with industry and many other fields, encouraging the exploration of new related technologies and AI. Due to the availability of cloud services and scalability for computing processes, individual users and organizations are transferring their applications, data and services to a cloud storage server. Despite its advantages, the transformation of on-premises computing to remote computing has brought many security issues and challenges for both the consumer and the provider. Many cloud services are provided by a third party, which creates new security threats. The cloud provider provides its services over the Internet and uses many web technologies, which creates security problems here as well. The study examines the main features of cloud technologies, security issues, potential threats and their solutions. Six key topics related to cloud security, cloud architecture framework, service and deployment models, cloud technologies, cloud security concepts, threats and attacks are described. The paper also discusses many open research questions related to risk assessment methods for each of the cloud vulnerabilities.*

*Dependence on cloud services is constantly growing, because more and more companies and organizations are switching to their use. This makes them more vulnerable to disruptions, cyber-attacks and other problems that can lead to significant data loss, financial losses and reputational losses.*

*Keywords: cloud services, vulnerabilities of cloud services, risk assessment of the use of cloud technologies, risk assessment methods.*

## Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями

Хмарні обчислення використовують великі обсяги віртуальної пам'яті для надання послуг на вимогу через Інтернет. Основними характеристиками хмарних обчислень є те, що користувачам не потрібно будувати дорогу обчислювальну інфраструктуру, а вартість послуг низька. В останні роки хмарні обчислення були інтегровані в промисловість та багато інших галузей, заохочуючи дослідників досліджувати нові суміжні технології. Завдяки доступності сервісів і масштабованості обчислювальних процесів окремі користувачі та організації переносять програми, дані та сервіси на сервери хмарних сховищ. Незважаючи на свої переваги, перехід від локального до віддаленого обчислення створює багато питань безпеки та викликів як для споживачів, так і для постачальників. Багато хмарних служб надаються перевіреними третіми сторонами та створюють нові загрози безпеці. Хмарні провайдери пропонують послуги через Інтернет і використовують

багато вебтехнологій, що створює нові проблеми безпеки.

У цій статті також обговорюється багато відкритих дослідницьких питань, пов'язаних із безпекою хмари. Огляд стану та тенденцій є важливим інструментом для організацій, які використовують або планують використовувати хмарні обчислення, надаючи чіткі вказівки щодо ідентифікації, оцінки та управління ризиками. Основні тенденції та аналітичні дослідження проводяться постійно, групи дослідників такі, як Gartner, Forrester та IDC (консалтингові компанії) визначають і публікують та висвітлюють поточний стан та тенденції в галузі безпеки хмарних даних та їх використання.

Хмарні сервери зберігають величезні обсяги чутливої інформації, що робить їх ласою здобиччю для кіберзлочинців. Дослідження ризиків кібербезпеки хмарних технологій є ключовим фактором для захисту даних та забезпечення їх конфіденційності. Хмарні технології постійно розвиваються, з'являються нові сервіси та функції, що може призвести до виникнення нових, непередбачуваних ризиків. Дослідження цих ризиків є актуальним оскільки дозволяє краще підготуватися до можливих проблем та мінімізувати їхні наслідки.

Європейське агентство з мережевої та інформаційної безпеки ( ENISA) публікує звіти та рекомендації щодо управління ризиками в хмарних обчисленнях, такі як "Cloud Computing Risk Assessment". Існують декілька методів оцінки ризиків щодо безпеки даних при використанні хмарних технологій. Основні з них [1].

1. Аналіз вразливостей (Vulnerability Assessment): Ідентифікація та оцінка вразливостей в системах і програмах, які можуть бути використані для кібератак.
2. Оцінка загроз (Threat Assessment): Визначення потенційних загроз, які можуть впливати на безпеку даних, включаючи кібератаки, природні катастрофи та людські помилки.
3. Аналіз наслідків (Impact Analysis): Оцінка можливих наслідків для бізнесу в разі порушення безпеки даних, включаючи фінансові втрати, шкоду репутації та юридичні наслідки.
4. Ризик-аналіз (Risk Analysis): Комбінований підхід, який включає оцінку вразливостей, загроз та наслідків для визначення загального рівня ризику для безпеки даних.
5. Аудит безпеки (Security Audit): Незалежна перевірка систем безпеки для виявлення можливих ризиків та невідповідностей встановленим стандартам і політикам.
6. Оцінка зрілості безпеки (Security Maturity Assessment): Визначення рівня зрілості чинних заходів безпеки та управління ризиками, порівняння з найкращими практиками в галузі.

У цій статті ми хочемо розглянути і проаналізувати ризики використання хмарних послуг з тим, щоб надалі обрати найбільш вдалі методи оцінки ризику для кожного з компонентів безпеки.

**Аналіз досліджень та публікацій**

Аналітична компанія MarketsandMarkets™ (рис. 1) опублікувала глобальне дослідження, в якому визначила ринкову частку хмарних послуг (cloud computing market share), а також тенденції ринку (cloud computing market trends). Згідно з зібраними даними, до 2029 року, розмір глобального ринку зросте до $118,5 млрд, якщо збережеться середньорічний темп приросту 27,1%. Для порівняння: у 2024 році ринкова частка склала $35,7 млрд [2].

Технологія хмарних послуг, крім збереження і надання доступу до даних, включає і сектор обчислень. Розширена аналітика еволюціонізує сектор хмарної аналітики, спрощуючи операції та покращуючи процеси прийняття бізнес-рішень. Ці платформи автоматизують завдання аналізу даних, використовуючи вдосконалене машинне навчання та алгоритми штучного інтелекту, забезпечуючи ефективне вилучення цінної інформації. Завдяки зручним інтерфейсам і бездоганній інтеграції з хмарними платформами розширені аналітичні рішення пропонують економічно ефективні та масштабовані варіанти для організацій будь-якого розміру. Прогнозне моделювання дозволяє підприємствам передбачати ринкові тенденції та завчасно приймати обґрунтовані стратегічні рішення. Застосування розширеної аналітики дозволяє компаніям залишатися попереду, використовуючи статистику на основі даних для стимулювання інновацій і максимального підвищення конкурентоспроможності у відповідних галузях.

Хмарні послуги застосовують у великій кількості сучасних бізнес-операцій. Вони мають попит завдяки численним перевагам: в першу чергу універсальності та гнучкості. Це призвело до впровадження рішень у різних галузях. Цьому сприяють служби Amazon S3, Google Cloud Storage та Microsoft Azure Blob Storage, які забезпечують безпечне й масштабоване зберігання всіх типів даних: документів та медіа. Використання хмарних технологій у різних країнах може призвести до необхідності дотримуватися певних норм та регуляцій, що стосуються захисту даних, конфіденційності та безпеки. Дослідження цих норм та їх впливу на хмарні сервіси теж є важливим для забезпечення законності та етичності їх використання.

Зростання використання хмарних технологій споживачами робить важливим дослідження ризиків, з якими вони можуть зіткнутися. Це дозволяє захистити їхні права та інтереси, забезпечити прозорість та чесність у наданні хмарних послуг. Глибоке розуміння ризиків хмарних технологій може дати компаніям конкурентну перевагу. Це дозволяє їм обирати найбезпечніші та найнадійніші рішення, мінімізувати ризики та максимізувати переваги хмарних технологій для свого бізнесу.

NIST (Національний інститут стандартів і технологій США): NIST розробив кілька стандартів і рекомендацій для безпеки хмарних технологій, зокрема NIST SP 800-144 "Guidelines on Security and Privacy in Public Cloud Computing" та NIST SP 500-292 "NIST Cloud Computing Reference Architecture". Основні з них наступні [3].

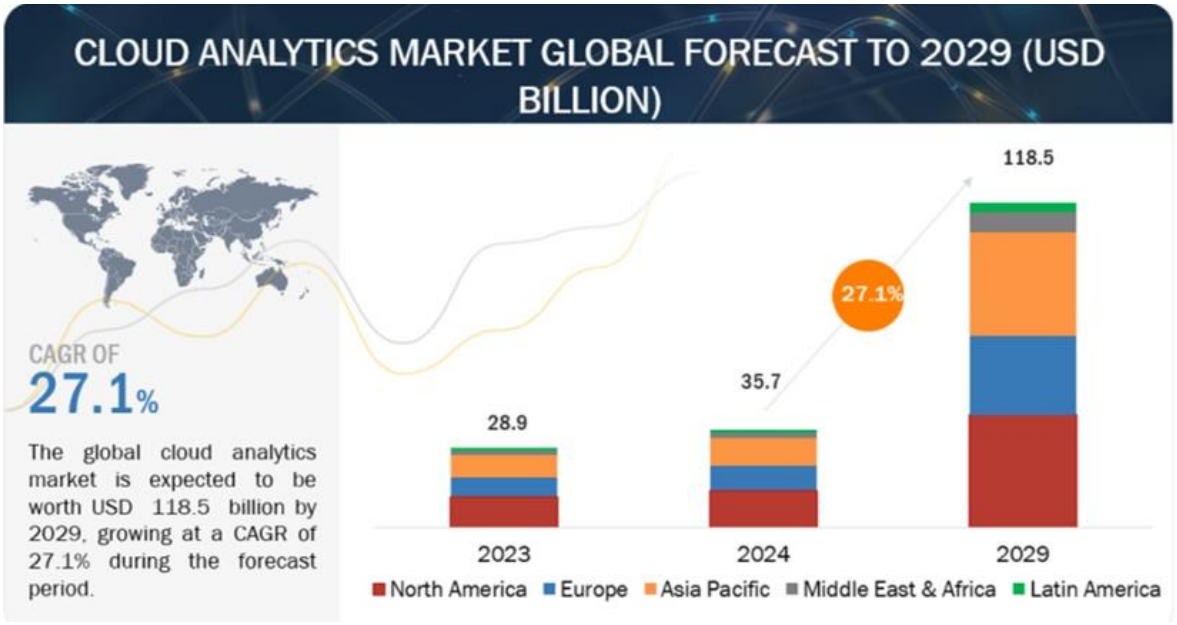


**Рис. 1. Дослідження аналітичної компанії MarketsandMarkets™ [2]**

**Шість ризиків використання хмарних технологій**

1. **Безпека даних:** дані в хмарі можуть бути вразливими до кібератак, витоків, або зловмисного доступу. Зашифровування, контроль доступу та постійний моніторинг є необхідними заходами для захисту даних.
2. **Втрата контролю** над даними: використання хмарних сервісів означає, що компанії передають контроль над своїми даними третій стороні. Це може стати проблемою, якщо постачальник хмарних послуг не дотримується потрібних стандартів безпеки або політик конфіденційності.
3. **Надійність постачальника:** Перебої в роботі або технічні проблеми з боку постачальника хмарних послуг можуть призвести до тимчасової недоступності даних або сервісів. Важливо вибирати надійних постачальників та мати плани на випадок аварій.
4. **Юридичні та регуляторні вимоги:** Хмарні послуги можуть підпадати під різні регуляторні вимоги та закони в залежності від місця розташування постачальника та користувача. Це може створювати додаткові юридичні ризики, особливо при зберіганні персональних даних.
5. **Продуктивність** та пропускна здатність мережі: Використання хмарних сервісів залежить від швидкості та надійності інтернет-з'єднання. Проблеми з мережею можуть впливати на продуктивність додатків та доступ до даних.
6. **Вартість:** Хмарні послуги можуть бути економічно вигідними, але неправильне управління ресурсами може призвести до непередбачених витрат. Необхідно ретельно планувати використання хмарних ресурсів і слідкувати за витратами, щоб уникнути перевитрат.

Хмарні обчислення пропонують гнучкий і масштабований підхід до надання IT-послуг за допомогою різних моделей обслуговування [4, 8]. Три основні моделі хмарних служб: програмне забезпечення як послуга (SaaS), платформа як послуга (PaaS) та інфраструктура як послуга (IaaS).

1 . Програмне забезпечення як послуга (SaaS):

SaaS – це служба хмарних обчислень, яка надає кінцевим користувачам доступ до програмних програм через Інтернет. Це позбавляє організацій від необхідності встановлювати, підтримувати та оновлювати програмне забезпечення локально. Натомість сторонній постачальник розміщує програми та робить їх доступними для користувачів на основі передплати. Популярні приклади SaaS включають інструменти управління взаємовідносинами з клієнтами (CRM), як-от Salesforce, платформи для співпраці, як-от Microsoft 365, і пакети продуктивності, як-от Google Workspace. SaaS спрощує керування програмним забезпеченням, знижує витрати та забезпечує віддалений доступ до програм, що робить його популярним вибором для компаній будь-якого розміру.

2. Платформа як послуга (PaaS):

PaaS – це служба хмарних обчислень, яка надає платформу, що дозволяє розробникам створювати, розгортати та керувати програмами, не маючи справу зі складнощами базової інфраструктури. Пропозиції PaaS включають інфраструктури розробки, бази даних і проміжне програмне забезпечення, що дозволяє розробникам зосередитися виключно на кодуванні та логіці програми. Це прискорює процес розробки, покращує співпрацю між командами розробників і забезпечує узгоджене середовище для розгортання програми. Прикладами постачальників PaaS є Heroku, Google App Engine і Microsoft Azure App Service.

3. Інфраструктура як послуга (IaaS):

IaaS – це служба хмарних обчислень, яка пропонує віртуальні обчислювальні ресурси через Інтернет. Він надає комплексний пакет інфраструктури, включаючи віртуальні машини, сховище та мережеві компоненти. IaaS дозволяє організаціям масштабувати свою IT-інфраструктуру відповідно до попиту, не інвестуючи у

фізичне обладнання. Ця гнучкість особливо корисна для підприємств із динамічним навантаженням або тих, хто прагне оптимізувати використання ресурсів. Серед провідних постачальників IaaS – Amazon Web Services (AWS), Microsoft Azure і Google Cloud Platform (GCP).

**Формулювання цілей статті**

**Метою роботи є** дослідження впливу шести ризиків використання хмарних сервісів і показати, які методів оцінки ризиків можна застосувати до оцінювання вразливостей хмарних послуг.

Залежність від хмарних сервісів постійно зростає, адже все більше компаній та організацій переходять на їх використання. Це робить їх більш вразливими до збоїв, кібератак та інших проблем, які можуть призвести до значних втрат даних, фінансових збитків та репутаційних втрат. У статті розглядаються основні особливості хмарних технологій, проблеми безпеки, потенційні загрози та їх вирішення. Описано шість ключових тем, пов'язаних із безпекою хмари, структуру хмарної архітектури, моделі обслуговування та розгортання, хмарні технології, концепції безпеки хмари, загрози та атаки. У дослідженні обговорюється багато відкритих дослідницьких питань, пов'язаних із методами оцінки ризиків до кожної з вразливостей використання хмари.

**Виклад основного матеріалу**

В одній статті розглянути усі ризики важко, тому зупинимось на шести основних.

Безпека даних: дані в хмарі можуть бути вразливими до кібератак.

Хмарна безпека важлива, оскільки використання хмари збільшує потенційну площу атаки – це відкриває нові шляхи для хакерів, щоб зламати вашу мережу. Використовуючи хмарні обчислювальні служби без належних заходів хмарної безпеки, ви надаєте зловмисникам можливості для викрадення даних, знищення конфіденційних файлів і несанкціонованого віддаленого входу у вашу систему. Хмарна безпека також є обов'язковою, якщо ваша організація зберігає персональні дані в хмарі. Згідно з вимогами більшості режимів захисту даних підприємства повинні вживати адекватних заходів для безпеки приватних даних, де б вони не зберігалися. Загальна відповідальність за втрату даних лежить на користувачі, а не на вашому постачальнику хмарних сервісів.

Деякі з останніх кіберзлочинних атак з 2021 років.

1. Colonial Pipeline (2021): Ця кіберзлочинна атака призвела до тимчасового закриття одного з найбільших трубопроводів нафти в Сполучених Штатах. Зловмисники використовували програмне забезпечення-вимагач, щоб заблокувати системи Colonial Pipeline і вимагати викупу.
2. Kaseya VSA (2021): Ця кіберзлочинна атака вразила понад 1500 компаній у 17 країнах. Зловмисники використовували програмне забезпечення для управління віддаленим доступом (RMM) Kaseya VSA, щоб встановити програмне забезпечення-вимагач на комп'ютери жертв.
3. Log4j (2021): Ця кіберзлочинна атака використовувала уразливість у бібліотеці Apache Log4j, яка використовується в багатьох програмних продуктах. Зловмисники могли використовувати цю уразливість для виконання довільного коду на комп'ютерах жертв.
4. CloudBreach (2022): Ця кіберзлочинна атака вразила понад 300 організацій, включаючи урядові органи, на підприємства та некомерційні організації. Зловмисники використовували хмарні сервіси для зберігання викрадених даних і вимагали викупу.
5. Conti (2022): Ця кіберзлочинна група є однією з найактивніших у світі. Conti здійснила численні атаки на організації в різних галузях, включаючи охорону здоров'я, енергетику та фінансові послуги.
6. Lapsus$ (2022): Ця кіберзлочинна група відома своїми атаками на високотехнологічні компанії. Lapsus$ використовувала різні методи для крадіжки даних і вимагання викупу, включаючи соціальну інженерію, фішинг та злом зламування.

Це лише кілька прикладів глобальних кібератак, які відбулися в останні роки. Кібератаки стають все більш досконалими та можуть завдати значної шкоди як приватним особам, так і організаціям.

Війну в Україні назвали першою в історії війною у кіберпросторі. Але ще задовго до повномасштабного вторгнення протистояння між Україною та росією набуло формату гібридної війни. Окрім економічних утисків, фінансування сепаратистів та неформального введення армії рф у Крим та на Донбас, війна тривала і у віртуальному вимірі. Росія ще до Майдану та Революції Гідності намагалася використовувати хакерські атаки, щоб заволодіти певною інформацією або як засіб політичного тиску. На відміну від інформаційних атак, що зосереджені на поширенні дезінформації, пропаганди або на впливі на громадську думку, кібервійна охоплює ширший спектр, як-от зломи систем, шпигунство, зараження шкідливим ПЗ, викрадення даних.

Важливо вживати заходів для захисту даних від кібератак, таких як

- Зашифровування даних: шифрування даних робить їх нечитабельними для зловмисників, навіть якщо вони отримують доступ до них.
- Контроль доступу: надання доступу до даних лише тим, кому він потрібен, може допомогти запобігти несанкціонованому доступу.
- Постійний моніторинг: постійний моніторинг мережі.

**Втрата контролю над даними**

У п'ятницю, 19 липня 2024 року о 04:09 UTC, у рамках регулярних операцій CrowdStrike випустив оновлення конфігурації вмісту для датчика Windows для збору телеметричних даних щодо можливих нових методів загроз. Ці оновлення є регулярною частиною механізмів динамічного захисту платформи Falcon. Проблемне оновлення конфігурації Rapid Response Content призвело до збою системи Windows. На хости Mac і Linux це не вплинуло [5].

З усього світу надходили повідомлення про масові збої в роботі комп'ютерних систем Crowdstrike, що використовуються для роботи авіакомпаній, банків, магазинів, лікарень і провідних ЗМІ. У світі скасували близько 1500 авіарейсів. Десятки тисяч людей застрягли в аеропортах, а деякі рейси екстрено приземлялись. Спостерігаються проблеми з потягами у Британії, з метро у Вашингтоні. Збій зачепив медичну систему Великої Британії. Керівник Tesla та X Ілон Маск заявив, що це найбільший IT збій за всю історію.

У Crowdstrike вибачилися перед клієнтами за це і повідомили, що відновлення систем може зайняти деякий час. Спочатку почали надходити повідомлення про те, що збій могло спричинити оновлення програмного забезпечення компанії Crowdstrike, яка виробляє антивірусне програмне забезпечення. Воно начебто блокує пристрої Windows, викликаючи так званий "синій екран смерті" на ПК.

Crowdstrike – це компанія з кібербезпеки, заснована в 2011 році для захисту найбільших світових компаній і обладнання від кіберзагроз і вразливостей. Вона спеціалізується на захисті кінцевих точок і намагається запобігти потраплянню шкідливого програмного забезпечення або файлів у корпоративні мережі з пристроїв, які до них підключаються, наприклад телефонів і ноутбуків. Вона також допомагає захистити дані компаній, які перенесли зберігання даних з власних серверів до так званих хмарних провайдерів. Техаську компанію заснували підприємці Джордж Курц, який залишається виконавчим директором, і Дмитро Альперович. У 2019 році вона публічно розмістила свої акції на технологічній фондовій біржі Nasdaq. З моменту свого запуску компанія відігравала ключову роль у розслідуванні кібератак.

*Збій зачепив і Україну.* Серед українських компаній про збої в роботі повідомляла Нова пошта, хоча пізніше в компанії заявили, що відновили роботу всіх клієнтських систем та сервісів. Проблеми також виникли у роботі monobank - у застосунку з'явилося повідомлення про складнощі у роботі деяких сервісів. Керівник компанії Олег Гороховський написав у телеграмі про глобальний IT-збій, проте не зазначив, чи саме він спричинив проблеми в роботі застосунку monobank. Про проблеми у роботі також кажуть і у ТАСКОМБАНК. За словами співробітників одного з київських відділень, багато операцій не проходять. У МОЗ запевняють, що ситуація не вплинула на роботу Helsi – медичної інформаційної системи України. В "Укрзалізниці" також розповіли, що все працює без збоїв.

Таким чином навіть найкращі можуть помилятись.

**Надійність постачальника**

В Україні представлені різні постачальники хмарних послуг, як міжнародні, так і локальні, ось деякі з них.

1. Microsoft Azure - глобальний постачальник хмарних послуг, який пропонує широкий спектр послуг, включаючи зберігання даних, аналітику, віртуальні машини та багато іншого.
2. Amazon Web Services (AWS) - ще один великий міжнародний гравець на ринку хмарних технологій, що надає різноманітні сервіси, такі як обчислення, зберігання, бази даних, аналітика.
3. Google Cloud Platform (GCP) - хмарні сервіси від Google, які включають віртуальні машини, бази даних, штучний інтелект, машинне навчання та багато інших сервісів.
4. De Novo - український постачальник хмарних послуг, який пропонує інфраструктуру як сервіс (IaaS), платформи як сервіс (PaaS) та інші хмарні рішення.
5. GigaCloud - українська компанія, що спеціалізується на наданні хмарних рішень для бізнесу, включаючи віртуальні сервери, зберігання даних, резервне копіювання тощо.
6. DataGroup - український телекомунікаційний оператор, що також надає хмарні сервіси, такі як віртуальні дата-центри, хмарні сховища, резервне копіювання та інші рішення.

Ці постачальники забезпечують різні рівні надійності та безпеки, тому важливо оцінювати їхні можливості, сервіси та рівень підтримки перед прийняттям рішення (табл.1).

Зведена таблиця з інформацією про рівні надійності основних постачальників хмарних послуг в Україні. У таблиці враховані такі параметри, як репутація на ринку, час безперебійної роботи (uptime), підтримка, і додаткові функції безпеки.

Таблиця 1

**Основні постачальники хмарних послуг в Україні**

| | **Постачальник** | **Час безперебійної роботи** | **Підтримка** | **Додаткові функції безпеки** |
|---|---|---|---|---|
| | В Україні | Відсоток часу, протягом якого сервіси залишаються доступними та працюють без збоїв. | Наявність технічної підтримки, її доступність та канали комунікації | Включають інструменти для шифрування даних, моніторинг, аудит та управління доступом. |
| | | | 24/7, мультиканальна | Шифрування даних, багаторівнева автентифікація, SIEM, DDoS-захист |
| | | | /7, мультиканальна | Шифрування даних, IAM, AWS Shield, CloudTrail, DDoS-захист |

| | Постачальник | Час безперебійної роботи | Підтримка | Додаткові функції безпеки |
|---|---|---|---|---|
| | | | 24/7, мультиканальна | Шифрування даних, Identity and Access Management (IAM), VPC Service Controls, DDoS-захист |
| | | | 24/7, технічна підтримка | Шифрування даних, багаторівнева автентифікація, резервне копіювання |
| | | | 24/7, технічна підтримка | Шифрування даних, багаторівнева автентифікація, резервне копіювання |
| | | | 24/7, технічна підтримка | Шифрування даних, багаторівнева автентифікація, резервне копіювання |

Юридичні та регуляторні вимоги: статистика за кількістю змін у законах з регулювання хмарних послуг.
Сполучені Штати:

- 2008: Закон про захист конфіденційності та безпеки даних у сфері охорони здоров'я (HIPAA) оновлено, щоб включити хмарні послуги.
- 2010: Закон про захист приватного життя в Інтернеті та законів про комунікації (COPPA) оновлено, щоб включити хмарні послуги.
- 2013: Закон про хмарні обчислення (Cloud Act) встановлює правила для зберігання даних уряду США в хмарних службах.
- 2018: Закон про захист даних для споживачів штату Каліфорнія (CCPA) встановлює правила для збору та використання особистої інформації споживачів.
- 2020: Закон про безпеку та захист даних (GDPR) Європейського Союзу (ЄС) застосовується до компаній, які обробляють особисті дані громадян ЄС, незалежно від того, де вони знаходяться.

Європейський Союз:

- 2002: Директива про електронні комунікації (eCom) встановлює правила для надання електронних комунікаційних послуг, включаючи хмарні послуги.
- 2016: Загальний регламент про захист даних (GDPR) встановлює правила для збору та використання особистої інформації громадян ЄС.
- 2022: Закон про цифрові послуги (DSA) та Закон про цифрові ринки (DMA) встановлюють правила для великих онлайн-платформ, включаючи хмарні послуги.

Україна:

- 2013: Закон України "Про захист персональних даних" встановлює правила для збору та використання особистої інформації в Україні.
- 2017: Закон України "Про електронні комунікації" встановлює правила для надання електронних комунікаційних послуг, включаючи хмарні послуги.
- 2021: Національна стратегія розвитку штучного інтелекту в Україні до 2025 року визнає хмарні послуги як ключову інфраструктуру для розвитку ШІ.

Важливо зазначити, що це лише деякі з ключових змін у законах, які впливають на хмарні послуги. Закони про хмарні послуги постійно розвиваються, і важливо стежити за останніми змінами, щоб гарантувати дотримання відповідності.

**Продуктивність та пропускна здатність мережі**

Національний інститут стандартів і технологій США (NIST) розробив кілька стандартів і рекомендацій для безпеки хмарних технологій, зокрема NIST SP 500-292 представляє референтну архітектуру для хмарних обчислень, що слугує стандартною моделлю для розуміння хмарних сервісів і їх компонентів [4, 7].
Основні пункти:

1. Компоненти архітектури: Опис основних компонентів хмарної архітектури, включаючи споживачів хмарних послуг, постачальників, брокерів, операторів та аудиторів.
2. Моделі розгортання: Роз'яснення різних моделей розгортання хмарних обчислень, таких як публічна, приватна, гібридна та спільна хмара.
3. Моделі сервісів: Визначення основних моделей сервісів у хмарних обчисленнях: IaaS, PaaS, SaaS.
4. Взаємодія компонентів: Опис способів взаємодії між різними компонентами хмарної архітектури для забезпечення надання хмарних послуг.
5. Функціональні аспекти: Пояснення функціональних можливостей хмарної архітектури, включаючи управління ресурсами, моніторинг, безпеку та конфіденційність.

6. Управління та політики: Вказівки щодо управління хмарними сервісами та політик, необхідних для забезпечення безпеки та відповідності регуляторним вимогам.
7. Приклади застосування: Практичні приклади використання референтної архітектури для розробки та впровадження хмарних рішень у різних галузях.

Параметри, які впливають на продуктивність та пропускну здатність мережі [6].

1. Пропускна здатність: це максимальна кількість даних, яку можна передати через мережу за одиницю часу. Пропускна здатність вимірюється в бітах за секунду (біт/с), мегабітах за секунду (Мбіт/с) або гігабітах за секунду (Гбіт/с).
2. Затримка: це час, необхідний для того, щоб пакет даних перейшов через мережу. Затримка вимірюється в мілісекундах (мс).
3. Пакетні втрати: це втрата пакетів даних під час їх передачі через мережу. Пакетні втрати зазвичай вимірюються у відсотках.
4. Ширина каналу: це діапазон частот, який використовується для передачі даних через мережу. Ширина каналу вимірюється в герцах (Гц).

Контроль цих параметрів.

- Моніторинг мережі: важливо постійно контролювати мережу, щоб виявляти та вирішувати проблеми, які можуть впливати на продуктивність.
- Управління пропускною здатністю: існує ряд методів управління пропускною здатністю, які можна використовувати для забезпечення того, щоб критичні додатки мали пріоритет у мережі.
- Оптимізація маршрутизації: важливо оптимізувати маршрутизацію трафіку в мережі, щоб мінімізувати затримку та втрату пакетів.
- Підвищення якості мережевого обладнання: використання високоякісного мережевого

Для кожного з ризиків, виявлених після оцінки ризику, потрібно прийняти рішення про відповідний метод обробки ризику. Можливі варіанти обробки ризиків включають впровадження належних механізмів контролю для зниження ризиків, прийняття ризиків при дотриманні умов та критеріїв прийняття ризиків, запобігання ризикам шляхом недопущення дій, які могли б викликати загрози, та передачу пов’язаних ризиків іншим сторонам (наприклад, страховикам або постачальникам). Зводячи разом методів оцінки ризиків та існуючи ризики використання хмарних технологій отримаємо дорожню карту для подальших досліджень. Описано шість ключових тем, пов’язаних із безпекою хмари, структуру хмарної архітектури, моделі обслуговування та розгортання, хмарні технології, концепції безпеки хмари, загрози та атаки.

**Основні моменти оцінки ризиків та їх зміст**

1. Ідентифікація ризиків.
    - Технічні ризики: Оцінка вразливостей, пов'язаних з інфраструктурою, програмним забезпеченням та мережевими компонентами.
    - Юридичні та нормативні ризики: Врахування вимог законодавства, контрактів і нормативних актів.
    - Організаційні ризики: Ризики, пов'язані з управлінням та організаційною структурою користувачів і постачальників хмарних послуг.
2. Категорії ризиків.
    - Конфіденційність: Ризики витоку або несанкціонованого доступу до конфіденційної інформації.
    - Цілісність: Ризики зміни або пошкодження даних.
    - Доступність: Ризики недоступності хмарних послуг або даних через технічні проблеми або атаки.
3. Методологія оцінки ризиків.
    - Аналіз загроз: Ідентифікація можливих загроз, таких як кіберзлочинність, технічні збої або природні катастрофи.
    - Аналіз вразливостей: Визначення слабких місць в хмарній інфраструктурі та додатках.
    - Оцінка наслідків: Оцінка потенційного впливу реалізації ризиків на бізнес, включаючи фінансові втрати та шкоду репутації.
4. Рекомендації щодо управління ризиками.
    - Технічні заходи: Впровадження заходів безпеки, таких як шифрування, багатофакторна автентифікація та безперервний моніторинг.
    - Організаційні заходи: Розробка політик безпеки, навчання персоналу та створення планів реагування на інциденти.
    - Контроль доступу: Управління правами доступу до хмарних ресурсів для мінімізації ризику несанкціонованого доступу.
5. Ролі та відповідальність.
    - Постачальники хмарних послуг: Обов'язки щодо забезпечення безпеки інфраструктури та послуг.
    - Користувачі хмарних послуг: Обов'язки щодо захисту даних та управління доступом до них.
6. Моніторинг та оцінка.

- Постійний моніторинг: Впровадження систем для постійного відстеження безпеки хмарних сервісів.
- Регулярна оцінка: Періодична перевірка ефективності заходів безпеки та оновлення політик відповідно до нових загроз і вимог.

**Висновки з даного дослідження і перспективи подальших розвідок у даному напрямі**

Ця стаття описує основні тенденції ризиків, проблеми безпеки, загроз та рішення у сфері хмарних технологій. Розглядаються теми, пов'язані з хмарою, а саме структури хмарної архітектури, моделі обслуговування та доставки, хмарні технології, концепції безпеки хмари, загрози та методи оцінки ризиків в залежності від категорій. Результатом дослідження є подання хмарних послуг як важливого інструменту для організацій, які використовують або планують використовувати хмарні обчислення або збереження даних, надаючи чіткі вказівки щодо ідентифікації, оцінки та управління ризиками. У статті розглянуті основні особливості хмарних технологій, проблеми безпеки, потенційні загрози та їх вирішення.

Дослідження ризиків хмарних технологій може стимулювати інновації в цій галузі. Це може призвести до розробки нових методів захисту даних, підвищення безпеки та надійності хмарних сервісів, а також до створення нових, більш безпечних та зручних хмарних рішень. Дослідження ризиків хмарних технологій сприяє стійкості та надійності хмарних сервісів. Це робить їх більш стійкими до кібератак, збоїв та інших проблем. Таким чином побільші дослідження є необхідними з точки зору розуміння і потреби забезпечити комплексну оцінку ризиків, пов'язаних з хмарними послугами, та надати рекомендації для їх мінімізації.

## References

1. European Union Agency for Network and Information Security. (2009). Cloud computing risk assessment. Retrieved from https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

2. Cloud Analytics Market by Offering ((Solutions (Advanced Analytics, Cloud Bl Tools), Deployment Mode (Public, Private, Hybrid)), Services), Data Type, Data Processing (Real-Time Analytics, Batch Analytics), Vertical and Region - Global Forecast to 2029. https://www.researchandmarkets.com/report/cloud-analytics

3. National Institute of Standards and Technology. (2011). Guidelines on security and privacy in public cloud computing (Special Publication 800-144). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-144.pdf

4. National Institute of Standards and Technology. (2011). NIST Cloud Computing Reference Architecture (Special Publication 500-292). Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

5. REMEDIATION AND GUIDANCE HUB: FALCON CONTENT UPDATE FOR WINDOWS HOSTS. https://www.crowdstrike.com/falcon-content-update-remediation-and-guidance-hub/

6. Singh, A., & Chatterjee, K. (2017). Cloud security issues and challenges: A survey. Journal of Network and Computer Applications, 79, 88-115. https://doi.org/10.1016/j.jnca.2016.11.027

7. Fuks, O., Ptashinsky, M. Ya., & Marikutsa, U. (2024). Study of methods for evaluating the quality of cloud services, including reliability, productivity and security metrics. Herald of Khmelnytskyi National University. Technical sciences, 335(3 (1)), 335-341.

8. Nikitina, L., Dzheniuk, N., & Borysova, L. (2024). Expert system for risk assessment of cloud services. Control, navigation and communication systems. Collection of scientific papers, 1(75), 146-151. https://doi.org/https://doi.org/10.26906/SUNZ.2024.1.146