Зибін Сергій Вікторович, доктор технічних наук, професор кафедри безпеки інформаційних технологій Національного авіаційного університету, Київ, Україна.
Serhii Zybin, Doctor of technical sciences, professor of the department of security of information technologies National Aviation University, Kyiv, Ukraine.
E-mail: zysv@ukr.net.
Orcid ID: 0000-0002-2670-2823.

Собчук Андрій Валентинович, доктор філософії, доцент кафедри інформаційної та кібернетичної безпеки, Навчально-науковий інститут Захисту інформації, Державний університет телекомунікацій, Київ, Україна.
Andrii Sobchuk, PhD, Associate Professor of the Department of Information and Cyber Security, Educational and Scientific Institute of Information Protection, State University of Information and Communication Technologies.
E-mail: anri.sobchuk@gmail.com.
Orcid ID: 0000-0003-3250-3799.

Ровда Володимир Володимирович, аспірант, Державний університет інформаційно-комунікаційних технологій.
Volodymyr Rovda, PhD student, State University of Information and Communication Technologies.
E-mail: volodymyr.rovda@gmail.com.
Orcid ID: 0009-0001-9987-6787.

DOI: 10.18372/2410-7840.26.18829
УДК 004.49

ДОСЛІДЖЕННЯ ТА АНАЛІЗ ПРОБЛЕМ ТА ВИКЛИКІВ, ЩО ВИНИКАЮТЬ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ В ХМАРНИХ ОБЧИСЛЕННЯХ

Марта Король, Іван Опірський

Хмарні сервіси передбачають надання інформаційним засобам віртуального середовища можливість розширити програмно-технічні ресурси комп'ютерного пристрою користувача. При цьому інформація постійно зберігається на серверах у мережі Інтернет та тимчасово кешується на пристроях клієнтів, таких як персональні комп'ютери, ігрові консолі, ноутбуки, смартфони тощо. Для отримання постійного доступу до віддалених інтернет-ресурсів користувачі використовують хмарні сервіси. Вони є ключовим елементом сучасних технологій, які швидко розвиваються, а для багатьох компаній використання хмарних сервісів є стратегічним питанням. Хоча інноваційні можливості хмарних сервісів з одного боку привертають увагу користувачів, але з іншого можуть створювати нові загрози для їхньої інформаційної безпеки. Саме тому дослідження хмарних обчислень є важливим для розуміння їхнього потенціалу та ефективності. У цьому дослідженні буде розглянуто аспект безпеки хмарних сервісів, та порівняння декількох різних платформ в цьому контексті, адже відсутність достатнього захисту може призвести до крадіжки персональних даних та іншої конфіденційної інформації. В дослідженні також будуть розглянуті найпоширеніші загрози, з якими зіштовхуються хмарні сервіси, такі як DDoS-атаки, витоки даних, зловживання даними тощо. Зокрема, будуть проаналізовані заходи захисту, які надають провідні хмарні платформи, такі як AWS, GCP та Azure, з метою визначення їхньої ефективності та надійності. Наш аналіз буде корисним як для компаній, які розглядають можливість переходу до хмарних технологій, так і для звичайних користувачів, які прагнуть зберегти безпеку своїх особистих даних в Інтернеті. Результати дослідження нададуть чітке уявлення про переваги та обмеження використання різних хмарних платформ з точки зору безпеки.
Ключові слова: *хмарні сервіси, AWS, AZURE, GCP, кібербезпека.*

ВСТУП

В сучасному цифровому світі, великі обсяги даних зберігаються та оброблюються в хмарних сервісах. Відомо, що хмарні сервіси надають безліч переваг, включаючи збільшення доступності, гнучкість та економічність. Проте, разом з цими перевагами приходить ряд викликів, таких як збільшення загроз безпеці, потенційна вразливість та потенційні ризики для конфіденційності даних.

На даний момент, на ринку хмарних обчислень відбувається зростанням конкуренції серед провайдерів хмарних сервісів. За останні роки спостерігається постійне збільшення кількості компаній, що пропонують хмарні послуги. Найбільш популярними з них є:

1. Amazon Web Services (AWS) [2], (створена у березні 2006р.), є підрозділом компанії Amazon.com, яка пропонує хмарну обчислювальну платформу в оренду для приватних осіб, компаній та урядів за підпискою;

2. Microsoft Azure (створена 1 лютого 2010 р.) [3] – це інфраструктура корпорації Microsoft, яка надає хмарну платформу для розробників додатків, з метою полегшення процесу створення онлайн програм. Microsoft Azure дозволяє розго-

ртати додатки не лише за допомогою Microsoft .NET і Visual Studio, але і з використанням різних інших інструментів;

3. Google Cloud Platform (засновано 7 квітня 2008 р.) [4]- набір хмарних служб, який був розроблений компанією Google, працює на тій же інфраструктурі, яку Google використовує для своїх продуктів, спрямованих на кінцевих користувачів. Сервіс надає ряд модульних хмарних служб, таких як обчислення, зберігання даних, аналіз даних та машинне навчання (рис. 1).

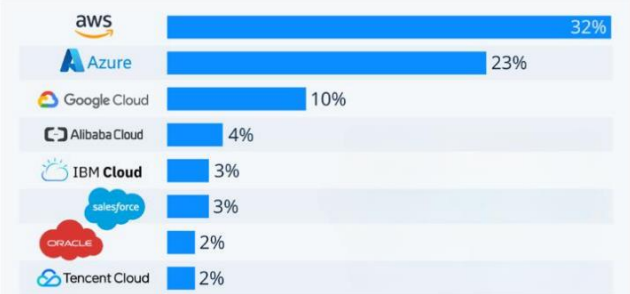

Рис. 1. Популярність постачальників хмарних послуг [5]

Зі зростанням популярності розробники змушені постійно вдосконалювати свої платформи, включаючи вдосконалення механізмів автоматичного виявлення та відповіді на загрози, розширення функцій шифрування даних, вдосконалення ідентифікації та автентифікації користувачів, а також вдосконалення інструментів моніторингу та аналізу вразливостей, Крім того, зростання конкуренції спонукає провайдерів хмарних послуг активніше співпрацювати з інформаційно-безпековими експертами, проводити незалежні аудити безпеки та вдосконалювати процеси реагування на інциденти.

Тема хмарних обчислень привертає увагу різних дослідників. Багато вчених та експертів активно займаються дослідженням та аналізом проблем та викликів, пов'язаних з забезпеченням кібербезпеки в хмарних обчисленнях. На приклад у роботі [6] розглядається забезпечення безпеки у обчислювальному сервіс AWS, вона демонструє важливість і актуальність досліджень у сфері кібербезпеки, зокрема в контексті використання хмарних сервісів AWS. Також у праці [7] автори порівняли сервіси AWS та Azure Cloud Platforms на 2021 рік, де визнають різницю між AWS і Azure щодо систем управління базами даних, архітектур, патернів управління ресурсами та складності, які можуть вплинути на масштабованість, продуктивність та ціноутворення.

Метою даного дослідження є аналіз та ідентифікація ключових проблем і викликів, що виникають у процесі забезпечення кібербезпеки в хмарних обчисленнях, за допомогою порівняння Amazon Web Services, Microsoft Azure, Google Cloud Platform. Для виконання даної буде виконано такі завдання:

- розглянути можливі загрози та ризики безпеки хмарних сервісів;
- розробити критерії оцінки безпеки в хмарних обчисленнях;
- протестувати AWS, AZURE, GCP в контексті обраних критеріїв забезпечення кібербезпеки;
- оцінити кожну платформу по 10-ти бальній системі;
- визначити яка з платформ є найкращою, та чому.

Таким чином, ретельне дослідження та аналіз проблем та викликів, пов'язаних з кібербезпекою в хмарних обчисленнях, стає надзвичайно важливим для розробки ефективних стратегій захисту даних.

ОСНОВНА ЧАСТИНА

Аналіз загроз та ризиків безпеки хмарних сервісів

Малі та середні підприємства, як і глобальні компанії, все більше покладаються на послуги безпеки хмарних обчислень для підтримки повсякденних бізнес-функцій, розробки програмного забезпечення і навіть для забезпечення технологічної інфраструктури, необхідної для роботи. У зв'язку з цим хмарні сервіси часто стикаються з багатьма кібератаками.

Хмарна атака [8] – це кібератака, націлена на платформи хмарних послуг, наприклад обчислювальні служби, служби зберігання або розміщені програми в моделі «платформа як послуга» (PaaS) або програмне забезпечення як послуга (SaaS).

За даними [9] в останні роки кількість атак на хмарні сервіси стрімко зросла. Кібератаки в області “хмар” становили 20% усіх кібератак у 2020 році, що зробило платформи хмарних обчислень третім найбільш цільовим кіберсередовищем. Саме тому ми розглянемо різні види атак та їх характеристики, а також можливі наслідки цих атак для користувачів і організацій, які використовують хмарні технології. Нижче наведено огляд 10 типів атак на хмарні обчислення, який допоможе краще зрозуміти ці загрози та вжити заходів для їх запобігання (рис. 2).

Ці загрози становлять серйозні ризики для безпеки хмарних обчислень. Атаки на відмову в обслуговуванні можуть призвести до перебоїв у доступі до хмарних сервісів, неправильна конфі-

гурація безпеки може відкрити двері для зловмисників, а атаки впровадження зловмисного програмного забезпечення в хмару загрожують конфіденційності та цілісності даних.

Рис. 2. Типи атак на хмарні обчислення

Хмарний криптомайнінг використовує ресурси хмарних обчислень для видобутку криптовалюти без дозволу власників, що може призвести до перевищення витрат та зниження продуктивності, викрадення облікового запису в хмарі, що означає несанкціонований доступ або контроль над обліковим записом хмарних обчислень зловмисником. Це може дозволити зловмиснику використовувати пов'язані ресурси для власних цілей або викрасти або маніпулювати даними, що зберігаються в хмарі.. Всі ці загрози потребують уважного моніторингу та вжиття відповідних заходів безпеки для захисту хмарних сервісів та даних користувачів.

Критеріїв оцінки кібербезпеки в хмарних обчисленнях

Враховуючи те, кібератаки стають все більш складними і загрози кібербезпеці постійно зростають, важливість розробки комплексної стратегії безпеки для хмарних сервісів стає необхідною. Для ефективного захисту від кібератак у хмарних сервісах рекомендується використовувати різноманітні заходи та методи захисту, що дозволяють гарантувати більш високий рівень безпеки для користувачів.

1. Розмежування доступу

Зважаючи, що AWS, Azure та Google Cloud - це провідні постачальники хмарних послуг, кожен з них має певні механізми для забезпечення кібербезпеки.

Одним з ключових механзімів є розмежування доступу та управління безпекою в середовищі хмарних обчислень.

Керування ідентифікацією та доступом (IAM) дозволяє створювати дозволи для ресурсів та керувати ними. IAM об'єднує контроль доступу до сервісів в єдину систему і є узгодженим набором операцій. Політики IAM містять роль, користувача або групу користувачів. Кожна роль містить у собі перелік дозволів.

Керування ідентифікаціє та доступом базується на таких принципах так як:

- багатофакторна автентифікація, котра додає додатковий рівень безпеки. Це означає, що для доступу до вашого облікового запису користувачеві потрібно буде підтвердити свою особистість за допомогою двох або більше методів автентифікації, таких як пароль та SMS-код;
- централізоване управління, за допомогою якого, користувачі можуть створювати та керувати політиками доступу для користувачів, груп та ролей з одного місця, що спрощує процес адміністрування;
- Role-based Access Control (RBAC) дозволяє визначати права доступу для користувачів на основі їхніх обов'язків та потреб. Це дозволяє точно налаштовувати доступ до ресурсів із врахуванням конкретних потреб вашої організації;
- IAM надає можливості аудиту та звітності, які дозволяють вести журнали подій доступу, аналізувати використання ресурсів та відслідковувати зміни політик доступу для відповідності регулятивним вимогам. Це дозволяє вам зберігати контроль над вашими даними та забезпечувати відповідність зі стандартами безпеки.

2. Захист від DDoS атак та інших мережевих загроз

Однією з найпоширеніших та найбільш загрозливих форм атак є DDoS (розподілений заперечення про обслуговування), які можуть спричинити значні завади в роботі мережі, призвести до втрати доступності сервісів та важливих даних, і навіть завдати значних фінансових втрат. Захист від DDoS атак відбувається на основі таких пунктів:

- масштабованість і еластичність інфраструктури;
- розподіленість;
- мережеві фільтри;
- оптимізація трафіку;
- служби моніторингу та аналітики.

3. Заходи для запобігання змінам даних без дозволу

У світі хмарних сервісів, де важлива безпека даних, запобігання несанкціонованим змінам інформації стає надзвичайно важливою задачею. Забезпечення конфіденційності даних вимагає впровадження ефективних заходів безпеки. У цьому контексті важливо розглянути заходи для запобігання змінам даних без дозволу, що стає основною складовою надійності та безпеки ін-

формації. У хмарних сервісах існує кілька функцій та механізмів, які допомагають уникнути змінам даних без дозволу:

- аудит та моніторинг: системи аудиту та моніторингу, які надаються хмарними постачальниками, дозволяють відстежувати всі дії з даними і ресурсами. Це допомагає вчасно виявляти потенційні загрози та незвичайну активність;

- шифрування даних: функції шифрування даних, такі як AWS Key Management Service, Google Cloud Key Management Service та Azure Key Vault, дозволяють захистити дані від несанкціонованого доступу, навіть якщо зловмисники отримають доступ до них;

- відслідковування змін: деякі хмарні сервіси надають можливість відслідковування змін у даних за допомогою журналів аудиту. Це дозволяє виявляти, хто, коли і які зміни були внесені до даних;

- резервне копіювання: функції резервного копіювання, які пропонуються хмарними постачальниками, дозволяють регулярно створювати копії даних і відновлювати їх у випадку несанкціонованих змін або втрати.

4. Модель спільної відповідальності

Модель спільної відповідальності - це концепція, яка визначає рівень відповідальності за безпеку і захист даних між хмарним сервісом та його клієнтами.

Ця модель визначає, хто відповідає за захист різних аспектів інфраструктури та даних у хмарному середовищі.

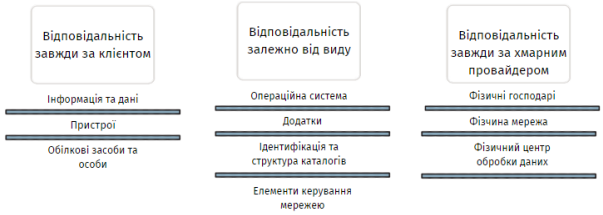

Рис. 3. Модель спільної відповідальності

Також платформи використовують 1 з 3-ох видів послуг: інфраструктуру як послугу (IaaS), платформу як послугу (PaaS), програмне забезпечення як послугу (SaaS).

SaaS[11] – це модель, яка покладає найбільшу відповідальність на постачальника хмарних послуг і найменшу на користувача. У середовищі SaaS ви відповідаєте за дані, які ви додаєте до системи, пристрої, яким ви дозволяєте підключатися до системи, і користувачів, які мають доступ.

Майже все інше належить хмарному провайдеру. Хмарний провайдер відповідає за фізичну безпеку центрів обробки даних, живлення, підключення до мережі, а також за розробку та оновлення програм.

PaaS [12] розподіляє відповідальність між вами та хмарним постачальником. Хмарний постачальник відповідає за підтримку фізичної інфраструктури та її доступ до Інтернету, як і в IaaS. У моделі PaaS хмарний провайдер також підтримуватиме операційні системи, бази даних та інструменти розробки. Подумайте про PaaS як про використання комп'ютера, приєднаного до домену: IT-спеціалісти обслуговують пристрій за допомогою регулярних оновлень, виправлень і оновлень.

IaaS [13] покладає на користувача найбільшу частку відповідальності. Хмарний провайдер відповідає за підтримку фізичної інфраструктури та її доступ до Інтернету. Ви несете відповідальність за встановлення та конфігурацію, виправлення та оновлення, а також безпеку.

5. Ефективність політик безпеки

Наявність та ефективність політик безпеки є однією з найбільш критичних аспектів. Правильно сконструйовані політики безпеки дозволяють забезпечити захист від широкого спектру загроз, від кібератак до несанкціонованого доступу та втрати даних.

Вони визначають правила, процедури та контрольні механізми, що регулюють доступ до інформації та ресурсів, а також встановлюють стандарти безпеки, які слід дотримуватися всіма користувачами та адміністраторами системи. У цьому контексті важливо дослідити як наявність, так і ефективність політик безпеки в хмарних сервісах, щоб забезпечити високий рівень захисту даних та інфраструктури.

Оцінка політики безпеки у хмарних сервісах включає ряд критеріїв, що дозволяють визначити її ефективність і адаптованість до вимог безпеки.

Деякі з ключових критеріїв оцінки включають:

- визначеність і консистентність;
- відповідність вимогам: політика безпеки повинна відповідати вимогам законодавства, стандартів та регуляторних вимог, які стосуються конкретної індустрії або регіону;
- моніторинг та аналіз;
- сталість та оновлення;
- підтримка та залучення працівників.

Оцінка політики безпеки за цими критеріями допомагає впевнитися, що вона відповідає потребам та вимогам безпеки у хмарних сервісах.

Проведення тестування кожної платформи відповідно до визначених критеріїв

Беручи до уваги критерії Критеріїв оцінки кібербезпеки в хмарних обчисленнях, які були складені у попередніх пунктах, ми здійснимо порівняння 3 хмарних сервісів: AZURE, AWS, GCP (табл. 1).

Таблиця 1

Порівняння платформу у контексті розмежування доступу

Особливість/ Сервіс	**AWS**	**AZURE**	**GCP**
Багатофакторна автентифікація	Так, підтримується через IAM та інші сервіси	Так, включаючи Azure AD та інші механізми	Так, доступно для користувачів та сервісів GCP через Identity Platform
Централізоване управління	Так, за допомогою Identity and Access Management (IAM)	Так, через Azure Active Directory (AAD) та інші інструменти	Так, з допомогою Cloud Identity and Access Management (IAM)
Role-based Access Control	Так, за допомогою IAM можна визначати ролі та надавати права доступу	Так, за допомогою Azure RBAC та інших механізмів	Так, доступно для налаштування прав доступу для користувачів та сервісів
Аудит та звітність	Так, надає можливості вести журнали подій та аналізувати використання ресурсів	Так, забезпечує можливості аудиту та звітності за допомогою Azure Monitor та інших інструментів	Так, надає можливості вести журнали подій та аналізувати доступ до ресурсів

Оцінюючи розмежування доступу для кожної з платформ (Azure, AWS, GCP) за шкалою від 1 до 10, де 10 – це найкраще, можна скласти такий рейтинг:

1. Azure (Microsoft Azure): 8. Сервіс має потужний і простий у використанні механізм керування доступом через Azure Active Directory (AAD). Він надає багато вбудованих ролей та можливостей керування, але деякі функціональності можуть бути складнішими у налаштуванні порівняно з іншими платформами;

2. AWS (Amazon Web Services): 9. IAM в AWS є потужним та гнучким інструментом для розмежування доступу. Він надає широкі можливості налаштування ролей, політик та доступу до API. Багато вбудованих ролей та можливостей дозволяють точно налаштувати доступ до ресурсів;

3. GCP (Google Cloud Platform): 7. IAM в GCP також є потужним інструментом з управління доступом, але він може бути менш гнучким у деяких аспектах порівняно з AWS та Azure. Проте, він надає розширений функціонал для керування проектами та ресурсами.

Тоді порівняємо платформи з точки зору захисту від DDoS атак та інших мережевих загроз (табл. 2).

Таблиця 2

Порівняння платформу у контексті захисту від DDoS атак та інших мережевих загроз

Особливість / Сервіс	**AWS**	**Azure**	**GCP**
Безкоштовний базовий рівень DDoS захисту	Так, доступно для всіх користувачів	Так, через Azure DDoS Protection	Ні
Розширений захист за додаткову плату	Так, доступно через AWS Shield Advanced	Ні, розширений захист недоступний за додаткову плату	Так, доступно через Google Cloud Armor та інші механізми
Web Application Firewall (WAF)	Так, AWS WAF	Ні, але є Azure Firewall та Azure Security Center	Так, Google Cloud Armor
Журнали подій та аналіз безпеки	Так, доступно через AWS CloudTrail та AWS Config	Так, доступно через Azure Security Center	Так, доступно через Google Cloud Security Command Center
Мережеве балансування навантаження	Так, доступно через AWS Elastic Load Balancer	Так, доступно через Azure Load Balancer	Так, доступно через Global Load Balancer та інші механізми
Мережеві правила та контроль доступу	Так, доступно через AWS Network ACLs та Security Groups	Так, доступно через Azure Firewall та Network Security Groups	Так, доступно через VPC Service Controls та інші механізми

Ознайомившись з платформами в аспекті захисту від DDoS атак та інших мережевих загроз, можна ми можемо надати їм такі оцінки:

1. AWS (Amazon Web Services): 9. AWS пропонує високий рівень захисту від DDoS атак та інших мережевих загроз, включаючи сервіси, такі як AWS Shield, AWS WAF, AWS Firewall Manager, Amazon GuardDuty та інші. Ці сервіси надають різні рівні захисту, як базовий, так і розширений, що дозволяє адаптувати заходи захисту до потреб користувачів. Багатофакторна аутентифікація, захист мережевих ресурсів та відстеження незвичайної активності також є складовими систем безпеки AWS;

2. Azure (Microsoft Azure): 8. Microsoft Azure також надає широкий спектр інструментів для захисту від DDoS атак та інших мережевих загроз, включаючи служби, такі як Azure DDoS Protection, Azure Firewall, Azure Application Gateway, Azure Security Center та багато інших. Azure має добре розвинуту систему моніторингу та виявлення загроз, що дозволяє швидко реагувати на потенційні атаки;

3. GCP (Google Cloud Platform): 7. Google Cloud Platform теж забезпечує значний рівень захисту від DDoS атак та інших мережевих загроз за допомогою сервісів, таких як Google Cloud Armor, Google Cloud DDoS Protection, VPC Service Controls та інші. Проте, на думку деяких фахівців, інструменти безпеки GCP можуть бути менш інтегрованими та менш простими у використанні порівняно з AWS та Azure, що може становити деякий ризик для користувачів з меншою експертизою у сфері безпеки мережі.

Нижче наведена таблиця, яка порівнює заходи для запобігання змінам даних без дозволу на платформах AWS, Azure та GCP за такими критеріями, як аудит та моніторинг, шифрування даних, відслідковування змін та резервне копіювання (табл. 3).

Таблиця 3

Порівняння платформу у контексті заходів для запобігання змінам даних без дозволу

Критерій / Платформа	AWS	Azure	GCP
Аудит та моніторинг	AWS CloudTrail, Amazon CloudWatch	Azure Monitor, Azure Security Center	Cloud Audit Logs, Cloud Monitoring
Шифрування даних	AWS Key Management Service (KMS), Amazon S3 Encryption	Azure Key Vault, Data Encryption at Rest	Key Management Service, Data Encryption at Rest
Відслідковування змін	AWS CloudTrail	Azure Audit Logs	Cloud Audit Logs
Резервне копіювання	Amazon S3, Amazon Glacier	Azure Backup	Google Cloud Storage, Cloud Storage Nearline

Розклад оцінок можна обґрунтувати так:

1. AWS (Amazon Web Services): оцінка 9. AWS має ряд потужних інструментів, таких як IAM для керування доступом, AWS KMS для шифрування даних, CloudTrail для аудиту та моніторингу, і Amazon S3 для резервного копіювання. Ці інструменти надають широкі можливості для захисту даних та високий рівень безпеки;

2. Azure (Microsoft Azure): оцінка 8. Azure також має схожий набір інструментів для захисту даних, таких як Azure Active Directory, Azure Key Vault, Azure Audit Logs та Azure Backup. Однак, деякі користувачі можуть вважати, що Azure трохи складніше в конфігурації та використанні, що може призвести до невеликої втрати балів у порівнянні з AWS;

3. GCP (Google Cloud Platform): оцінка 7. GCP також має деякі ефективні інструменти для захисту даних, але може бути менш гнучким у деяких аспектах порівняно з AWS та Azure. Хоча інструменти, такі як Cloud IAM, Key Management Service та Cloud Audit Logs, пропонують високий рівень безпеки, інтерфейс та документація GCP можуть бути менш інтуїтивними для деяких користувачів, що призводить до зниження загального оцінки. Далі буде розглянуто аспект моделі спільної відповідальності (табл. 4):

1. Azure (Microsoft Azure): 9. Azure надає чітко визначену модель спільної відповідальності, яка визначає, за які частини інфраструктури відповідає хмарний провайдер, а за які - користувач. Це допомагає уникнути плутанини та розуміти відповідальність кожної сторони за безпеку даних та інфраструктури;

2. GCP (Google Cloud Platform) 8. GCP також надає докладну модель спільної відповідальності,

але деякі користувачі вважають, що деякі аспекти можуть бути менш очевидними або складнішими для розуміння порівняно з Azure або AWS.

3. AWS (Amazon Web Services): 9. AWS має добре визначену та докладну модель спільної відповідальності, що дозволяє користувачам чітко розуміти їхню відповідальність за безпеку та захист даних у хмарному середовищі.

Таблиця 4

Порівняння платформу у контексті моделей спільної відповідальності

Аспект / Платформа	**Amazon Web Services (AWS)**	**Microsoft Azure**	**Google Cloud Platform (GCP)**
Інструменти та сервіси	AWS Identity and Access Management (IAM), AWS Shield, AWS WAF та інші сервіси для керування безпекою та захистом	Azure Active Directory (AAD), Azure DDoS Protection та інші сервіси для керування безпекою та захистом	Google Cloud IAM, Google Cloud Armor, Google Cloud Security Command Center (SCC) та інші сервіси для керування безпекою та захистом
Моделі послуг	IaaS, PaaS та SaaS	IaaS, PaaS та SaaS	IaaS, PaaS та SaaS
Політики безпеки та стандарти	AWS використовує власні політики безпеки та стандарти, такі як PCI DSS, HIPAA, SOC, ISO.	Azure використовує власні політики безпеки та стандарти, такі як PCI DSS, HIPAA, SOC, ISO.	GCP використовує власні політики безпеки та стандарти, такі як PCI DSS, HIPAA, SOC, ISO та інші.

Таблиця 5

Порівняння платформу у контексті ефективності політик безпеки

Аспект / Платформа	**Amazon Web Services (AWS)**	**Microsoft Azure**	**Google Cloud Platform (GCP)**
Наявність сертифікатів	SOC 1, SOC 2, ISO 27001, HIPAA, PCI DSS, FedRAMP	SOC 1, SOC 2, ISO 27001, HIPAA, PCI DSS, FedRAMP	SOC 1, SOC 2, ISO 27001, HIPAA, PCI DSS, FedRAMP
Підтримка віртуалізації	AWS Config, AWS Inspector, AWS Trusted Advisor.	Azure Security Center, Azure Policy, Azure Firewall.	Google Cloud Security Command Center, Google Cloud IAM, Google Cloud Armor.

Оцінка ефективності політик безпеки в різних хмарних платформах може бути наступною (табл. 5):

1. Azure (Microsoft Azure) 9. Azure надає широкі можливості для створення та налаштування політик безпеки через Azure Security Center та Azure Policy. Завдяки цим сервісам, адміністратори можуть ефективно контролювати та моніторити стан безпеки ресурсів у хмарному середовищі Azure. Azure також надає можливості для інтеграції з іншими системами моніторингу та управління безпекою, що підвищує його ефективність;

2. GCP (Google Cloud Platform) 8. GCP також має широкий набір інструментів для налаштування політик безпеки, включаючи Cloud Security Command Center та Google Cloud IAM. Однак, деякі користувачі можуть вважати, що інтерфейс користувача та документація GCP можуть бути менш інтуїтивно зрозумілими порівняно з Azure або AWS, що може ускладнити встановлення та налагодження політик безпеки;

3. AWS (Amazon Web Services) 9. AWS пропонує широкий спектр інструментів для створення та керування політиками безпеки, включаючи AWS Identity and Access Management (IAM), AWS Config, AWS CloudTrail, і багато інших. Ці сервіси дозволяють адміністраторам ефективно контролювати та моніторити безпеку ресурсів у хмарному середовищі AWS.

З наданих оцінок, можна зазначити, що Amazon Web Services (AWS) набув найвищої загальної оцінки, яка складає 45 балів. Це є суб'єктивна думка яка будувалась на основі того то того, що AWS вирізняється в плані технічних аспектів завдяки своїй широкій набір послуг, глибокому рівню налаштування та високій географічній розгалуженості. Найбільшою перевагою AWS є потужний та гнучкий інструментарій для розмежування доступу, а також широкий спектр інстру-

ментів для захисту від DDoS атак та інших мережевих загроз. Враховуючи це, можна зробити висновок, що AWS є найкращим вибором для організацій, які надають пріоритет безпеці в хмарних обчисленнях.

Таблиця 6

Підсумки порівняння

Аспект / Платформа	AWS	AZURE	GCP
Розмежування доступу	9	8	7
Захист від DDoS атак та інших мережевих загроз	9	8	7
Заходи для запобігання змінам даних без дозволу	9	8	7
Моделі спільної відповідальності	9	9	8
Ефективність політик безпеки	9	9	8
Загальна оцінка	45	42	37

ВИСНОВКИ

На основі проведеного дослідження та аналізу проблем та викликів, пов'язаних з забезпеченням кібербезпеки в хмарних обчисленнях, можна зробити кілька ключових висновків.

В першу чергу, виявлено, що захист від кіберзагроз у хмарних обчисленнях вимагає комплексного та глибокого підходу, оскільки ці області надають широкий спектр послуг та можливостей, які вимагають постійного моніторингу та управління. До ключових викликів в цьому контексті належать забезпечення безпеки та захисту даних, виявлення та відповідь на кіберзагрози, а також управління доступом та ідентифікацією користувачів.

Другим важливим аспектом є необхідність постійного оновлення та удосконалення заходів безпеки, оскільки кіберзагрози постійно еволюціонують та стають все більш складними. Це означає, що провайдери хмарних обчислень, такі як AWS, Azure та GCP, повинні постійно вдосконалювати свої інструменти та сервіси, щоб забезпечити найвищий рівень безпеки для своїх клієнтів.

Крім того, виявлено, що вибір платформи для хмарних обчислень може впливати на рівень кібербезпеки, оскільки кожен провайдер має свої унікальні особливості та можливості. Вирішальним фактором при виборі платформи повинна бути її здатність надавати надійний та ефективний захист від кіберзагроз у відповідності до потреб та вимог конкретної організації.

Отже, на основі цих висновків можна стверджувати, що забезпечення кібербезпеки в хмарних обчисленнях є складним завданням, але водночас відкриває широкі можливості для інновацій та розвитку. З розумінням та своєчасним реагуванням на проблеми та виклики цієї області, організації можуть максимально забезпечити безпеку своїх даних та інфраструктури в хмарних середовищах.

ЛІТЕРАТУРА

[1]. Cloud services, Pharmaceutical Encyclopedia, 2022 [електронний ресурс]. https://www.pharmencyclopedia.com.ua/article/7857/xmarni-servisi 11 березня 2024.

[2]. Amazon Web Services, Wikipedia, 2023 [електронний ресурс]. https: // uk. wikipedia.org/ wiki/Amazon_Web_Services. Дата доступу: 11 березня 2024.

[3]. Microsoft Azure, Wikipedia, 2024 [електронний ресурс] https: //uk.wikipedia.org / wiki/Microsoft_ Azure. Дата доступу: 11 березня 2024.

[4]. Google Cloud Platform, Wikipedia, [електронний ресурс]. https: // uk.wikipedia.org / wiki / Google_ Cloud_Platform. Дата доступу: 15 березня 2024.

[5]. Felix Richter, (2024). Worldwide market share of leading cloud infrastructure service providers. https:/ /www.statista.com/chart/18819/worldwide-market-share-of-leading-cloud-infrastructure-service-providers.

[6]. Mazur V. M., (2023). Assessment of the security of the use of cloud technologies and the development of methods of protection against cyber-attacks on cloud services. https: //elartu.tntu.edu.ua/handle/lib /41631.

[7]. Yassin Maleh, Youssef Baddi, Mamoun Alazab, Loai Tawalbeh, (2021). Cybersecurity Analysis: Investigating the Data Integrity and Privacy in AWS and Azure Cloud Platforms. https: //link.springer.com/chapter /10.1007/978-3-030-74575-2_17.

[8]. Amit Sheps, 2023. Top 10 Cloud Attacks and What You Can Do About Them. https: // www.aquasec. com/cloud-native-academy/ cloud-attacks/cloud-attacks/.

[9]. "Cloud cyber-attacks: The latest cloud computing security issues" triskele Labs, [електронний ресурс]. https://www.triskelelabs.com/blog/cloud-cyber-attacks-the-latest-cloud-computing-security-issues. Дата доступу: 25 березня 2024.

[10]. "What is Azure RBAC" Learn Microsoft, [електронний ресурс]. https: // learn.microsoft.com/en-us/training/ modules / secure-azure-resources-with-rbac/2-rbac-overview. Дата доступу: 28 березня 2024.

[11]. "SaaS" Learn Microsoft, [електронний ресурс]. https://learn.microsoft.com/en-us/training/modu-

les/describe-cloud-service-types/4-describe-software-service. Дата доступу: 1 квітня 2024.
[12]. "PaaS" Learn Microsoft, [електронний ресурс]. https://learn.microsoft.com/en-us/training/modules/describe-cloud-service-types/3-describe-platform-service. Дата доступу: 1 квітня 2024.
[13]. "IaaS" Learn Microsoft, [електронний ресурс]. https://learn.microsoft.com/en-us/training/modules/describe-cloud-service-types/2-describe-infrastructure-service. Дата доступу: 1 квітня 2024.

RESEARCH AND ANALYSIS OF PROBLEMS AND CHALLENGES IN ENSURING CYBERSECURITY IN CLOUD COMPUTING

Cloud services provide information tools in a virtual environment with the ability to expand the software and hardware resources of a user's computer device. In this case, the information is permanently stored on servers on the Internet and temporarily cached on client devices, such as personal computers, game consoles, laptops, smartphones, etc. To get constant access to remote Internet resources, users use cloud services. They are a key element of modern and rapidly developing technologies, and for many companies, the use of cloud services is a strategic issue. Although the innovative capabilities of cloud services attract the attention of users on the one hand, they can also pose new threats to their information security. That is why the study of cloud computing is important to understand its potential and effectiveness. This study will examine the security aspect of cloud services and compare several different platforms in this context, as the lack of sufficient protection can lead to theft of personal data and other confidential information. The study will also look at the most common threats faced by cloud services, such as DDoS attacks, data leaks, data misuse, etc. In particular, we will analyze the security measures provided by leading cloud platforms such as AWS, GCP and Azure to determine their effectiveness and reliability. Our analysis will be useful both for companies considering moving to the cloud and for ordinary users seeking to keep their personal data safe online. The results of the study will provide a clear picture of the benefits and limitations of using different cloud platforms from a security perspective.

Keywords: cloud services, AWS, AZURE, GCP, cyber security.

Король Марта Ярославівна, студентка кафедри захисту інформації Національного університету «Львівська політехніка».
Marta Korol, student at the Department of Information Security, Lviv Polytechnic National University.
E-mail: marta.korol.kb.2022@lpnu.ua.
Orcid ID: 0009-0002-8079-1799.

Опірський Іван Романович, д.т.н., професор, завідувач кафедри захисту інформації Національного університету «Львівська політехніка».
Ivan Opirskyy, Doctor of Technical Sciences, Professor, Head of the Department of Information Security, National University "Lviv Polytechnic".
E-mail: ivan.r.opirskyi@lpnu.ua.
Orcid ID: 0000-0002-8461-8996.

DOI: 10.18372/2410-7840.26.18830
УДК 004.49

ВИКЛИКИ ТА МОЖЛИВОСТІ КІБЕРБЕЗПЕКИ В ІНТЕРНЕТІ РЕЧЕЙ (IOT): ПОЄДНАННЯ ШТУЧНОГО ІНТЕЛЕКТУ, IOT ТА КІБЕРБЕЗПЕКИ

Олександр Улічев, Роман Яровий, Костянтин Задорожний

Метою роботи є дослідження викликів та можливостей, пов'язаних з кібербезпекою в контексті інтернету речей (IoT) та поєднанням штучного інтелекту (ШІ) з IoT, відомим як AIoT. Робота розглядає еволюцію IoT до AIoT, важливість кібербезпеки в AIoT та різноманітні виклики, що виникають у зв'язку зі збільшенням кількості підключених до мережі пристроїв та зростанням обсягу даних. Дослідження також розглядає стратегії кібербезпеки для AIoT, включаючи захист мережевого зв'язку, використання штучного інтелекту в системах виявлення та запобігання кібератак, контроль доступу та ідентифікацію, а також оперативний моніторинг та виявлення аномалій. В статті розглядається питання стандартизації та регулювання в галузі AIoT-кібербезпеки та майбутні напрями розвитку в цій галузі, зокрема приділено увагу напрямкам: використання блокчейн-технологій, розширення ролі штучного інтелекту в кібербезпеці AIoT. Заключна частина статті містить висновки дослідження, рекомендації щодо подальших досліджень та вдосконалення кібербезпеки в AIoT.

***Ключові слова**: інтернет речей (IoT), штучний інтелект, аномалії трафіку, штучний інтелект речей(AIoT), кібербезпека, дерева рішень, K-найближчі сусіди, машини опорних векторів.*

ВСТУП

Інтернет речей стрімко розвивається, сьогодні кількість пристроїв в мережі оцінюється десятками мільярдів – починаючи від побутових домашніх пристрої, закінчуючи агрегатами промислового виробництва та спеціальними пристроями в прикладних галузях (наука, освіта, медицина). За прогнозами електронного видання Statista [15], кількість пристроїв Інтернету речей (IoT) у світі майже подвоїться з 15,1 мільярда у 2020 році