5. SpiderFoot. OSINT Automation Tool. URL: https://www.spiderfoot.net (дата звернення: 20.04.2025).
6. GitHub-репозиторій Recon-ng. URL: https://github.com/lanmaster53/recon-ng (дата звернення: 20.04.2025).

Ключові технології кібербезпеки хмарного середовища

УДК 004.056.5:004.08
Артем Роженко[1], Ігор Аверічев[2]
Державний університет інформаційно-комунікаційних технологій,
[1]a.rozhenko@stud.duikt.edu.ua, [2]iaverichev19@gmail.com

З розвитком цифрових технологій та збільшенням доступу до Інтернету, організації стають вразливими до різних видів кібератак та мережевим вторгненням. Поширені проблеми включають складність розуміння, обмеження в роботі з масивними наборами даних, тривалий час обробки, значні вимоги до зберігання та підвищений рівень помилок.

Хмарні обчислення в Інтернеті речей (IoT) виникли як революційна парадигма, яка глибоко вплинула на безліч сфер, включаючи системи охорони здоров'я, військові програми, освіту тощо. Його привабливість походить від притаманної йому економічності та надзвичайної надійності, що дозволяло організаціям масштабувати свої операції з безпрецедентною гнучкістю. Однак із зростанням залежності від хмарної інфраструктури виникла зловісна та постійна загроза кібератак [1]. Постійні кібератаки та мережеві вторгнення на цифрову інфраструктуру порушують нормальну роботу системи, здійснюючи зловмисні дії, що порушують цілісність даних, конфіденційність, доступність і конфіденційність.

У відповідь на цю зростаючу загрозу посилення безпеки хмарних мереж стало першорядним. Зважаючи на ці виклики, у центрі уваги цього дослідницького заходу – сприяти розробці оптимізованої, зручної стратегії захисту хмарних систем від кіберзагроз. Використовуючи силу інновацій, мета полягає в тому, щоб подолати розрив між зростаючою складністю сучасних кіберзагроз і потребою в ефективних, зрозумілих і ефективних рішеннях безпеки для хмарних екосистем [2].

Крім того, хмарні обчислення надають послуги в Інтернеті, які стали широко використовуваною технологією. Модель хмарних обчислень розвинулась із технології віртуалізації, розподілених обчислень, службових обчислень та інших комп'ютерних технологій, щоб забезпечити функції доступності та масштабованості для великих програм корпоративного рівня. Він також пропонує послуги для віртуальних машин, призначених через значний пул фізичних ресурсів.

Хмарні обчислення пропонують кілька переваг для різних хмарних моделей на основі тенденцій безпеки та проблем. А саме включаючи зниження витрат, спільне використання та налаштування обчислювальних ресурсів, обслуговування на вимогу, а також високу гнучкість і масштабованість, швидке керування, економічна продуктивність, велика ємність пам'яті та переваги швидкого доступу до кінцевих пристроїв у будь-який час і всюди [3].

Перелічимо п’ять життєво важливих особливостей хмарних обчислень включають самообслуговування на вимогу, розширений доступ до мережі, об’єднання ресурсів, високошвидкісну відмовостійкість і вимірювані послуги. Ці переваги спонукають великі компанії переносити свою IT-інфраструктуру в хмарне середовище [4].

Для надійних послуг хмарні обчислення мають бути захищені для даних користувачів. Хмарні обчислення стикаються з кількома типовими хмарними ризиками, такими як зловживання даними, зловмисники, незахищені інтерфейси, точки доступу, спільні технологічні проблеми, втрата даних і викрадення. Тому точне розуміння хмарної безпеки є фундаментальною вимогою для успішного розгортання хмарних обчислень.

Різні типи атак ускладнюють хмарним провайдерам і адміністраторам розгортання можливих рішень, необхідних клієнтам [4]. Це пояснюється тим, що різні атаки пов’язані з різними загрозами, де важливість ризиків змінюється залежно від потреб безпеки інших клієнтів, які використовують хмарні служби.

Таким чином, адміністратори безпеки оцінять і впровадять механізми безпеки, щоб відповідати основним вимогам безпеки як постачальників послуг. Однак безпеку можна покращити, оскільки на практиці практично неможливо налаштувати повністю безпечну систему [5]. Отже, необхідно знайти загрози безпеці, а потім відповідні рішення, такі як підзвітність, автентифікація та збереження конфіденційності.

Однак багато питань безпеки заважають прийняттю хмарних обчислень. Тому існує гостра потреба в рішеннях безпеки для боротьби з різними загрозами безпеці в хмарних обчисленнях.

1. Halim, Z.; Sulaiman, M.; Waqas, M.; Aydın, D. Deep neural network-based identification of driving risk utilizing driver dependent vehicle driving features: A scheme for critical infrastructure protection. J. Ambient. Intell. Humaniz. Comput. 2023, 14, 11747–11765. [Google Scholar] [CrossRef].

2. Butt, U.A.; Amin, R.; Mehmood, M.; Aldabbas, H.; Alharbi, M.T.; Albaqami, N. Cloud security threats and solutions: A survey. Wirel. Pers. Commun. 2023, 128, 387–413. [Google Scholar] [CrossRef].

3. Falowo O.I., Botsyoe L., Koshoedo K., Ozer M. (2024). Enhancing cybersecurity with artificial immune systems and general intelligence: A new frontier in threat detection and response. IEEE Access.

4. Nafea, R.A.; Almaiah, M.A. Cyber security threats in cloud: Literature review. In Proceedings of the 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 14–15 July 2021; pp. 779–786. [Google Scholar].

5. Alotaibi, A.F. A comprehensive survey on security threats and countermeasures of cloud computing environment. Turk. J. Comput. Math. Educ. (TURCOMAT) 2021, 12, 1978–1990. [Google Scholar].