КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2025.27.773
УДК 004.862

Хомчак Михайло Вікторович
аспірант
Державний університет «Київський авіаційний інститут», Київ, Україна
ORCID ID: 0009-0000-4127-556X
mykhailo.khomchak@gmail.com

ОЦІНКА РИЗИКІВ КІБЕРБЕЗПЕКИ ДЛЯ ВИБОРУ ХМАРНОГО ПРОВАЙДЕРА

Анотація. У статті представлено розробку модуля оцінки ризиків кібербезпеки для вибору постачальника хмарних послуг, що дозволяє організаціям обґрунтовано вибирати постачальників, враховуючи всі аспекти безпеки. Модуль розроблений як частина комплексної системи підтримки прийняття рішень (DSS) і використовує детальну таксономію хмарних послуг, що охоплює різноманітні моделі та варіанти розгортання (IaaS, PaaS, SaaS, публічні, приватні та гібридні хмари). Створена система здійснює оцінку безпеки на основі зібраних даних про вразливості, що включають інформацію з Національної бази даних вразливостей (NVD) та інших джерел. Одним із основних етапів оцінки є визначення ризиків, пов'язаних з кожною послугою, що дозволяє точно виявити потенційні загрози та обрати постачальника, який має найкращі показники безпеки. Модуль оцінює різні фактори, включаючи частоту та критичність вразливостей, можливість їх експлуатації зловмисниками, а також швидкість усунення вразливостей. Зібрані дані дозволяють формувати зважену матрицю оцінки ризиків, яка допомагає приймати рішення на основі конкретних критеріїв. Результати дослідження показують, що розроблений модуль може значно покращити процес вибору постачальника хмарних послуг, особливо для великих організацій, що мають високі вимоги до безпеки даних. Подальші дослідження передбачають інтеграцію цього модуля в автоматизовані системи підтримки прийняття рішень, що дозволить адаптувати процес вибору постачальника до динамічного розвитку хмарних технологій і нових загроз.

Ключові слова: хмарні технології; хмарні обчислення; публічна хмара; вибір постачальника хмарних послуг; оцінка ризиків кібербезпеки.

ВСТУП

Швидка еволюція хмарних обчислень кардинально змінила підходи, якими організації керують своїми даними та розгортають додатки. Міграція на хмарні інфраструктури відкриває безпрецедентні можливості для масштабування, операційної гнучкості та економії витрат. До 2024 року понад 50% даних, що належать 753 організаціям, дослідженим компанією Flexera, розміщено в публічних хмарних середовищах. Малі та середні бізнеси є найбільшими користувачами хмари, з 61% навантаження та 60% даних у публічній хмарі [1]. 2023 рік став першим, коли управління витратами на хмарні послуги стало головним викликом для всіх організацій, що досліджувались, обігнавши безпеку [2]. Таким чином, оскільки бізнеси все більше покладаються на численні хмарні сервіси, проблема ефективного вибору партнера значно ускладнюється та стає критичною.

Разом з перевагами, такими як масштабованість, операційна гнучкість і економія витрат, виникає низка ризиків, які можуть поставити під загрозу конфіденційність, цілісність і доступність критичних бізнес-активів. Організації повинні враховувати численні фактори — включаючи вартість, продуктивність, безпеку та надійність [3] — щоб переконатися, що обраний постачальник не лише відповідає поточним вимогам, а й здатний адаптуватися до майбутніх викликів.

Серед цих викликів кібербезпека є однією з найбільш актуальних проблем для організацій, які прагнуть обрати хмарного постачальника послуг. Порушення конфіденційності, цілісності та доступності даних не тільки шкодять репутації організації, а й можуть призвести до фінансових збитків, штрафів та небажаних юридичних наслідків. Більш того, з поширенням кіберзагроз — від атак програм-вимагачів до витоків даних і складних постійних загроз (advanced persistent threats, APT) — важливість включення оцінки ризиків кібербезпеки до процесу вибору хмарного постачальника послуг не можна недооцінювати.

Постановка проблеми. Проблема, з якою стикаються організації при виборі хмарного постачальника послуг, полягає в складності та мінливості кібербезпекових ризиків, пов'язаних з впровадженням хмари. Крім того, швидка еволюція хмарних технологій та різноманітність моделей хмарних послуг (IaaS, PaaS, SaaS [4]) ускладнюють процес оцінки стану безпеки потенційних хмарних постачальників. Багато організацій стикаються з проблемою відсутності стандартизованих методологій оцінки ризиків і труднощами отримання прозорих, порівнянних та дієвих даних щодо безпеки від постачальників.

Більше того, організації часто не здатні належним чином оцінити весь спектр ризиків, пов'язаних з хмарними послугами, таких як вразливості в основній хмарній інфраструктурі, специфічні для постачальника засоби безпеки та відповідність нормативним вимогам. Як наслідок, вони можуть неефективно вибрати постачальників з недостатніми заходами безпеки або не впровадити необхідні міри зменшення ризиків. Відсутність комплексної та структурованої оцінки створює значні труднощі для організацій, які прагнуть приймати обґрунтовані рішення щодо вибору хмарного постачальника, який відповідає найкращим практикам та забезпечує необхідний рівень захисту.

Аналіз останніх досліджень і публікацій. Вибір оптимального постачальника хмарних послуг (CSP) з точки зору впливу ризиків інформаційної безпеки є предметом багатьох досліджень. У цьому підрозділі здійснюється аналіз робіт, що вивчають оцінку ризиків кібербезпеки, включаючи дослідження, які використовують різні моделі підтримки прийняття рішень, фреймворки, що описують безпеку хмарних сервісів та методології для вибору CSP на основі профілів їх ризиків. Ці роботи допомагають прояснити різноманітні підходи до оцінки CSP та розуміння складнощів хмарної безпеки.

Критичний огляд [5] аналізує кілька досліджень, присвячених викликам безпеки хмарних обчислень, зокрема, витокам даних, проблемам конфіденційності та сегрегації даних. У дослідженні запропоновані такі рішення, як використання шифрування, цифрових підписів і технологій блокчейн для вирішення цих проблем. Автор підкреслює важливість врахування цих аспектів забезпечення безпеки при виборі постачальника хмарних послуг (CSP).

Автори дослідження [6] провели систематичний огляд застосування машинного навчання (ML) для покращення безпеки хмарних обчислень. Вони виділили методи машинного навчання, такі як опорні вектори (SVM) та методи кластеризації, для виявлення загроз безпеці хмари, включаючи атаки типу Distributed Denial-of-Service (DDoS) та порушення конфіденційності даних. Оскільки кількість організацій, що впроваджують хмари зростає, автори наголошують на важливості інтеграції передових технологій, таких як ML, у процеси оцінки ризиків експлуатації хмарних послуг для виявлення, мінімізації та запобігання потенційним атакам.

У дослідженні [7] розглядаються проблеми безпеки хмари, вивчаючи загрози, що виникають для хмарних інфраструктур, транспортування даних та підключень клієнтів до хмарних послуг. У своїй статті вони пропонують використовувати Систему оцінки загроз за допомогою загальних вразливостей (CVSS) для пріоритетного вирішення цих проблем безпеки. Дослідження наголошує на тому, як розуміння вразливостей та оцінка ризиків, пов'язаних із цими вразливостями, може допомогти CSP впроваджувати кращі заходи безпеки. Аналіз на основі CVSS надає структурований метод для кількісної оцінки критичності загроз.

Дослідження [8] обговорює проблеми безпеки хмари та представляє методологію покращення безпеки хмарних послуг. У дослідженні розглядаються різні техніки, такі як управління ідентифікацією та доступом (IAM), шифрування даних і безперервний моніторинг для забезпечення цілісності даних у багатокористувацьких хмарних архітектурах. Автор підкреслює для постачальників хмарних послуг необхідність впроваджувати надійні безпекові фреймворки для зменшення нових загроз, таких як DDoS-атаки та витоки даних.

У контексті вибору хмарної платформи в роботі [9] представлена математична модель, інтегрована в систему підтримки прийняття рішень (DSS) для вибору хмарних платформ на основі нечіткої логіки та теорії ігор. Модель авторів враховує такі фактори, як інвестиції, безпека та якість послуг, надаючи обчислювально здійсненний спосіб збалансувати ці аспекти при виборі хмарної платформи. Ця методологія допомагає відповідальним особам, що приймають рішення, аналізувати компроміси між ризиками безпеки, якістю послуг та фінансовими інвестиціями, що є критично важливим для організацій зі складними потребами в безпеці.

Важливим внеском є робота [10], де дослідники запропонували модель оцінки ризиків прийняття хмарних технологій (CARAM), інструмент для оцінки ризиків, пов'язаних з впровадженням хмарних обчислень. CARAM інтегрує дані з кількох джерел, включаючи постачальників хмарних послуг та клієнтів, і використовує багатокритеріальний підхід до прийняття рішень для порівняння та ранжування постачальників хмарних послуг на основі їхніх профілів ризиків. Ця модель підкреслює важливість оцінки ризиків безпеки, конфіденційності та доставки послуг перед вибором постачальника хмарних послуг, пропонуючи структуровану методологію для осіб, які приймають рішення, щоб зрозуміти та зменшити потенційні ризики.

Дослідження [11] зосереджуються на оцінці безпеки постачальників хмарних послуг, використовуючи опитувальник Consensus Assessment Initiative Questionnaire (CAIQ) від Cloud Security Alliance (CSA). У їхньому дослідженні запропоновано автоматизовану систему для спрощення процесу порівняння безпеки, використовуючи відповіді CSP на питання CAIQ для ранжування їх можливостей із забезпечення безпеки. Дослідження підкреслює важливість безпеки як основного критерію вибору CSP і пропонує практичний підхід до порівняння безпеки серед різних постачальників.

У роботі [12] відзначається, що хмарні середовища за своєю природою є складними та динамічними, що ускладнює оцінку ризиків кібербезпеки традиційними методами, які ґрунтуються на статичних критеріях та періодичних ручних аудитах, які швидко застарівають через високу динаміку змін у каталогах послуг хмарних провайдерів та появою нових вразливостей. Як наслідок, ці методи можуть не охоплювати весь спектр ризиків, залишаючи організації вразливими до кіберзагроз.

Мета статті. Метою цієї статті є розробка модуля оцінки ризиків кібербезпеки, що буде використовуватися у процесі прийняття рішень у комплексній системі вибору постачальника хмарних послуг, що найкраще відповідає потребам організації.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Структура модуля оцінки ризиків кібербезпеки для вибору CSP

Модуль оцінки ризиків кібербезпеки для вибору хмарного провайдера розроблений як частина комплексної системи прийняття рішення для вибору хмарного провайдера, шляхом оцінки безпекових ризиків, пов'язаних з різними хмарними послугами. Модуль включає кілька компонентів, які разом забезпечують всебічну, об'єктивну та орієнтовану на дані оцінку постачальників хмарних послуг в контексті інформаційної безпеки.

Назви компонентів та опис кроків по оцінці ризиків відображено на рис. 1.

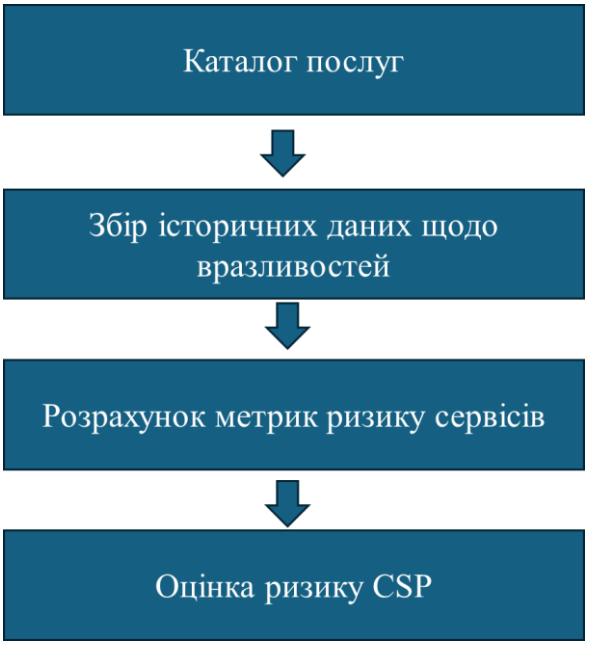

Рис. 1. Структура модуля оцінки ризиків.

Таксономія та каталог хмарних послуг

В основі модуля оцінки ризиків кібербезпеки для вибору CSP лежить таксономія сучасних публічних хмарних послуг [13], яка надає ієрархічний каталог усіх запропонованих послуг. Ця таксономія охоплює весь спектр моделей хмарних послуг (інфраструктура як послуга, платформа як послуга, програмне забезпечення як послуга) та варіанти розгортання (публічні, приватні, гібридні, спільні хмари). Основні категорії послуг включають обчислювальні ресурси, зберігання даних, мережі, бази даних, інструменти для розробників, аналітику, штучний інтелект/машинне навчання, безпеку, Інтернет речей та багато інших, кожна з яких поділяється на підкатегорії та послуги, що надаються конкретними постачальниками. Наприклад, у категорії обчислювальних ресурсів підпослуги включають віртуальні машини (наприклад, AWS EC2, Azure VMs, Google Compute Engine) та сервіси контейнерів/Kubernetes (наприклад, AWS EKS, Azure AKS, Google Kubernetes Engine). У категорії зберігання таксономія включає об'єктне зберігання (AWS S3, Azure Blob Storage тощо), а також блочне зберігання та файлові системи.

Такий всеохоплюючий каталог забезпечує виявлення та категоризацію всіх хмарних послуг, які може використовувати організація від початку впровадження. Використовуючи таксономію у якості меню вибору послуг CSP, модуль дозволяє користувачам ввести конкретні хмарні послуги, які вони планують використовувати.

Наприклад, користувач може вибрати послуги, такі як «Обчислення — Віртуальні машини», «Обчислення — Оркестрація контейнерів» і «Зберігання — Об'єктне зберігання», якщо їх хмарна архітектура базуватиметься на віртуальних машинах, кластерах Kubernetes і об'єктних сховищах. Посилаючись на таксономію, модуль забезпечує чітке визначення цих виборів (включаючи конкретні імена послуг постачальників) і гарантує, що жоден важливий компонент не буде проігноровано.

Будуючи оцінку ризиків навколо категорій послуг (замість того, щоб робити це лише на рівні постачальника), модуль надає детальнішу інформацію, визнаючи, що постачальник хмарних послуг може мати сильні сторони в забезпеченні певних послуг, але мати більше вразливостей в інших. Це також відповідає кращим практикам інвентаризації активів (у цьому випадку активів хмарних послуг) як першому кроку в управлінні ризиками.

Зазначимо, що широке охоплення таксономії IaaS, PaaS і SaaS означає, що модуль можна застосовувати до будь-якої хмарної операційної моделі. Незалежно від того, чи планує організація впровадження IaaS (лише віртуальні машини), чи PaaS (наприклад, керована база даних або служба оркестрації контейнерів), чи SaaS-додаток, ці послуги будуть відображатися в таксономії та будуть включені в оцінку. Модуль також розрізняє моделі розгортання — наприклад, публічний хмарний сервіс віртуальної машини порівняно з приватним хмарним (локальним) гіпервізором — вказуючи контекст у таксономії. Даний аспект є важливим, оскільки профілі ризиків можуть відрізнятися: у публічному хмарному IaaS постачальник хмарних послуг забезпечує базову інфраструктуру, а клієнт — операційну систему та додатки, тоді як у приватній хмарі, де використовується та сама технологія, клієнт несе повну відповідальність за інформаційну безпеку. Оцінюючи потреби організації відповідно до таксономії послуг, модуль відслідковує нюанси відповідальності та контролю за безпекою в кожному сценарії.

Збір історичних даних щодо вразливостей

Після того, як користувач вибирає хмарні послуги, які підлягають оцінці, модуль автоматично збирає історичні дані про вразливості, що стосуються цих послуг. Це здійснюється через інтеграцію з Національною базою даних вразливостей NIST (NVD) [14], яка каталогізує публічно розкриті CVE (Common Vulnerabilities and Exposures) разом із показниками їхньої критичності. Модуль прив'язує кожну вибрану хмарну послугу до відповідних програмних/апаратних продуктів та запитує NVD щодо їхніх минулих вразливостей. У багатьох випадках ризик хмарної послуги пов'язаний з базовою технологією або платформою, яку вона використовує. Наприклад:

- Служби віртуальних машин (IaaS) — відповідні CVE можуть включати вразливості гіпервізорів (наприклад, помилки Xen або VMware ESXi, якщо постачальник хмарних послуг використовує їх) або інструменти управління віртуалізацією.
- Служби оркестрації контейнерів — модуль збирає CVE для технологій, таких як Kubernetes, Docker та систем оркестрації контейнерів, оскільки керовані послуги Kubernetes часто успадковують вразливості цих платформ.
- Служби хмарного зберігання — вразливості можуть включати проблеми з API об'єктного зберігання або файловими протоколами зберігання.
- Служби управління та IAM — модуль також перевіряє вразливості в консолях управління хмарами, фреймворках управління ідентифікацією та доступом (IAM) тощо.

Для кожного відповідного запису CVE, модуль аналізує ключові атрибути: дата, опис, вразливий продукт та оцінки критичності. Використовується базовий бал CVSS (Common Vulnerability Scoring System) [15], наданий NVD, як міра критичності. Оцінки CVSS коливаються від 0 до 10 і відображаються у вигляді якісних рейтингів критичності:

- CVSS = 9.0–10.0 — критична;
- CVSS = 7.0–8.9 — висока;
- CVSS = 4.0–6.9 — середня.

Ці оцінки вказують на те, наскільки критичними можуть бути наслідки вразливості, якщо вона буде використана.

Окрім базової критичності, модуль також враховує частоту та історію вразливостей для кожної послуги. Це включає кількість розкритих CVE за період 5 років для технологій, на яких побудована послуга, і як часто з'являються Критичні/Високі вразливості. Модуль також враховує можливість експлуатації вразливості та терміни усунення вразливостей за даними NVD.

Додатково модуль оцінює зрілість рішення в контексті усунення вразливостей: як швидко CSP або постачальник програмного забезпечення випустив патчі або інструменти мітигації ризиків після повідомлення про вразливість, вчасність інформування клієнтів, Модуль також використовує тимчасові метрики CVSS, такі як Exploit Code Maturity та Remediation Level.

Модуль збирає необхідну інформацію про вразливості для кожної послуги та будує профіль безпеки для кожної вибраної послуги, який включає:

- кількість CVE за останній час;
- відсоток проблем з високою критичністю (CVSS ≥7);
- найгіршу спостережену оцінку CVSS;
- наявність exploits;
- середній час до виправлення.

На наступному кроці ці сирі дані використовуються для оцінки ризику.

Метрики ризику

Використовуючи зібрані дані про вразливості, модуль оцінює кожну послугу за допомогою рейтингу ризику (Низький, Середній, Високий). Цей рейтинг визначається на основі комбінації факторів, що відповідають найкращим практикам оцінки ризиків, які враховують як ймовірність інцидентів, так і їхній вплив:

- частота — вірогідність повторного виникнення нових подібних вразливостей на основі історичних даних;
- вплив — критичність потенційних наслідків, визначається за балами CVSS;
- експлуатованість — можливість використати ці вразливості зловмисниками.
- зрілість в усуненні вразливостей — оцінка ефективності та швидкості усунення вразливостей.

Кожна послуга оцінюється за усіма цими вимірами. Модель використовує зважену формулу:

$$S_i = \frac{F_i \times C_i \times E_i}{R_i},$$

де S_i — рейтинг ризику, F_i — частота, C_i — вплив, E_i — експлуатованість, R_i — зрілість в усуненні для кожної послуги.

Кожен фактор оцінюється за шкалою від 1 до 5. Вищий бал означає вищий ризик. Методологія призначає наступні числові значення:

$$F_i = \begin{cases} 1, \text{якщо} < 5\ CVE \text{ за 5 років} \\ 2, \text{якщо} \gg 5\ CVE < 10\ CVE \text{ за 5 років} \\ 3, \text{якщо} \gg 10\ CVE < 25\ CVE \text{ за 5 років} \\ 4, \text{якщо} \gg 25\ CVE < 15\ CVE \text{ за 5 років} \\ 5, \text{якщо} > 50\ CVE \text{ за 5 років} \end{cases}$$

$$C_i = \begin{cases} 1, \text{якщо нема критичних вразливостей} \\ 2, \text{якщо критичних вразливостей} \gg 1\ < 5 \text{ за 5 років} \\ 3, \text{якщо критичних вразливостей} \gg 5 < 10 \text{ за 5 років} \\ 4, \text{якщо критичних вразливостей} \gg 10 < 15 \text{ за 5 років} \\ 5, \text{якщокритичних вразливостей} > 15 \text{ за 5 років} \end{cases}$$

$$E_i = \begin{cases} 1, \text{якщо немає експлойтів} \\ 2, \text{якщо кількість експлойтів} \gg 1\ CVE < 5 \text{ за 5 років} \\ 3, \text{якщо кількість експлойтів} \gg 5\ < 10 \text{ за 5 років} \\ 4, \text{якщо кількість експлойтів} \gg 10 < 15 \text{ за 5 років} \\ 5, \text{якщокількість експлойтів} > 15 \text{ за 5 років} \end{cases}$$

$$R_i = \begin{cases} 1, \text{якщо швидкість виходу патчу чи іншої мітигації} < 5 \text{ днів} \\ 2, \text{якщо швидкість виходу патчу чи іншої мітигації} \gg 5 \text{ днів} < 10 \text{ днів} \\ 3, \text{якщо швидкість виходу патчу чи іншої мітигації} \gg 10 \text{ днів} < 25 \text{ днів} \\ 4, \text{якщо швидкість виходу патчу чи іншої мітигації} \gg 25 \text{ днів} < 45 \text{ днів} \\ 5, \text{якщо швидкість виходу патчу чи іншої мітигації} > 50 \text{ днів} \end{cases}$$

Рейтинг ризику кожного обраного провайдера хмарних послуг розраховується на наступному кроці.

Зважена матриця прийняття рішень для оцінки ризику CSP

Після оцінки окремих послуг, структура об’єднує результати в зважену матрицю прийняття рішень для оцінки сумарного ризику кожного постачальника хмарних послуг. Матриця структурована наступним чином:

- перелік необхідних сервісів до впровадження;
- вага кожної послуги, що визначається об’ємом послуг у загальному портфелі необхідних послуг у %;
- рейтинг ризик для кожної послуги впровадженні у кожного постачальника хмарних послуг.

Загальний рейтинг ризику визначається як загальнозваженний рейтинг ризику усіх послуг.

Приклад даної оцінки надано у табл. 1.

Таблиця 1

Зважена матриця прийняття рішень для оцінки ризику CSP

Сервіс	Вага	Provider 1	Provider 2	Provider 2
Compute (VMs)	30%	Низький = 1	Низький = 1	Високий = 3
Containers (K8s)	30%	Середній = 2	Високий = 3	Середній = 2
Storage (Object)	20%	Низький = 1	Низький = 1	Низький = 1
Database (Managed SQL)	20%	Середній = 2	Високий = 3	Середній = 2
Загальний рейтинг ризику	100%	Низький = 1.5	Середній = 2	Середній = 2.1

Визначення кандидатів на постачальників здійснюється користувачем. Модуль створює матрицю, яка порівнює цих постачальників.

Обчислення оцінок ризику постачальника хмарних послуг здійснюється для кожного CSP. Розраховується зважена оцінка як сума (оцінка ризику послуги × вага послуги) по всіх вибраних послугах. Це дає сумарну оцінку ризику для постачальника. Нижчі бали означають нижчий загальний ризик.

Зважена матриця прийняття рішень для оцінки ризиків CSP об’єднує всю аналітику в одному вигляді. Вона надає обґрунтоване, орієнтоване на дані порівняння. Під час перевірок управління або аудиту ця матриця може продемонструвати, що вибір постачальника CSP був здійснений з належною увагою до оцінки ризиків інформаційної безпеки.

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У результаті проведеного дослідження розроблено модуль оцінки ризиків кібербезпеки для вибору постачальника хмарних послуг, який включає комплексний підхід до аналізу безпекових характеристик хмарних послуг, їх вразливостей і потенційних загроз. Модуль орієнтований на організації, що прагнуть ефективно інтегрувати хмарні технології в свою інфраструктуру, зокрема для великих організацій, де вибір постачальника має важливе значення для збереження інформаційної безпеки.

Модуль оцінки ризиків передбачає збирання і аналіз даних про вразливості різних хмарних послуг, застосування таксономії для класифікації послуг, а також розробку зваженої матриці для прийняття рішень. Це дозволяє організаціям отримати чітке та структуроване уявлення про ризики, пов’язані з використанням конкретних хмарних сервісів, та вибрати найбільш безпечного та відповідного постачальника.

Подальшим напрямком дослідження є створення методології та розробка комплексної системи прийняття рішень щодо обґрунтованого вибору постачальника хмарних послуг для великих підприємств. Важливим кроком є інтеграція цього модуля в комплексну систему підтримки прийняття рішень (DSS) для автоматизації процесу вибору постачальника хмарних послуг. Цей модуль стане частиною більшої системи, яка враховуватиме різноманітні бізнес-вимоги та специфікації, що дозволяє покращити точність і ефективність процесу вибору в реальному часі. У майбутньому буде розширено базу даних для збору інформації про нові вразливості та постачальників хмарних послуг, що дозволить забезпечити актуальність та точність оцінки ризиків.

Подальші дослідження будуть зосереджені на вдосконаленні методів прогнозування нових кіберзагроз з використанням алгоритмів машинного навчання та на розробці більш динамічних методів оцінки безпеки, що враховуватимуть швидко змінювані умови хмарних середовищ.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Luxner, T. (2024). *Cloud computing trends: Flexera 2024 State of the Cloud Report. Flexera.* https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/
2. Luxner, T. (2023). *Cloud computing trends and statistics: Flexera 2023 State of the Cloud Report. Flexera.* https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2023-state-of-the-cloud-report/
3. Khomchak, M. (2024). Enterprise private cloud platforms: A systematic review of key vendors. *International Journal of Wireless and Microwave Technologies, 14(4),* 1–14. https://doi.org/10.5815/ijwmt.2024.04.01
4. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology, 53(6),* 50.
5. Al-Otaibi, S. Z. (2022). Data Security Challenges and Solutions in Cloud Computing: Critical Review. *Communications in Mathematics and Applications, 13(2),* 795.
6. Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. *IEEE Access, 9,* 20717–20735.
7. Süß, F., Freimuth, M., Aßmuth, A., Weir, G. R., & Duncan, B. (2024). *Cloud security and security challenges revisited.* arXiv preprint arXiv:2405.11350.
8. Vaka, P. R. (n.d.). *Cloud Security: Challenges, Methodologies, And Future Directions*.
9. Makulov, K., Chikrii, À., Lakhno, V., Yagaliyeva, B., Malyukov, V., Malyukova, I. N. N. A., & Lakhno, M. (2025). Cloud Platform Selection Model in the Framework of Differential Quality Game with Fuzzy Information. *IEEE Access*.
10. Cayirci, E., Garaga, A., Santana de Oliveira, A., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. *Journal of Cloud Computing, 5(1),* 14.
11. Pape, S., Paci, F., Jürjens, J., & Massacci, F. (2020). Selecting a Secure Cloud Provider—An Empirical Study and Multi Criteria Approach. *Information, 11(5),* 261.
12. Da Silva, C. A., Ferreira, A. S., & de Geus, P. L. (2012). A methodology for management of cloud computing using security criteria. *2012 IEEE Latin America Conference on Cloud Computing and Communications (LatinCloud),* 49–54. https://doi.org/10.1109/LatinCloud.2012.6508157
13. Khomchak, M. (2024). A Comprehensive Taxonomy of Modern Public Cloud Services for Infrastructure Selection. *International Journal of Computing, 23(3),* 468–475. https://doi.org/10.47839/ijc.23.3.3667
14. *National vulnerability database (NVD).* (2025). NIST. https://www.nist.gov/programs-projects/national-vulnerability-database-nvd
15. *National vulnerability database (NVD).* (2025). NIST. https://www.nist.gov/programs-projects/national-vulnerability-database-nvd
16. *Vulnerability metrics: CVSS. National Vulnerability Database.* (n.d.). National Institute of Standards and Technology. https://nvd.nist.gov/vuln-metrics/cvss

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 3 (27), 2025
ISSN 2663 - 4023

Mykhailo Khomchak
PhD Student
State University "Kyiv Aviation Institute", Kyiv, Ukraine
ORCID ID: 0009-0000-4127-556X
mykhailo.khomchak@gmail.com

CYBERSECURITY RISK ASSESSMENT FOR SELECTING A CLOUD SERVICE PROVIDER

Abstract. This paper presents the development of a cybersecurity risk assessment module for selecting a cloud service provider, enabling organizations to make informed decisions based on all aspects of security. The module is designed as part of an integrated decision support system (DSS) and utilizes a detailed taxonomy of cloud services, covering various models and deployment options (IaaS, PaaS, SaaS, public, private, and hybrid clouds). The system performs security assessments based on collected vulnerability data, including information from the National Vulnerability Database (NVD) and other sources. One of the key stages of the assessment is determining the risks associated with each service, which allows for the accurate identification of potential threats and the selection of a provider with the best security performance. The module evaluates various factors, including the frequency and severity of vulnerabilities, the likelihood of exploitation by attackers, and the speed of vulnerability remediation. The collected data is used to form a weighted risk assessment matrix that aids decision-making based on specific criteria. The results of the study show that the developed module can significantly improve the cloud service provider selection process, particularly for large organizations with high data security requirements. Future research will focus on integrating this module into automated decision support systems, which will allow the selection process to be adapted to the rapidly changing conditions of cloud technologies and emerging threats.

Keywords: cloud technology; cloud computing; public cloud; cloud service provider selection; cybersecurity risk assessment.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Luxner, T. (2024). *Cloud computing trends: Flexera 2024 State of the Cloud Report. Flexera.* https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/
2. Luxner, T. (2023). *Cloud computing trends and statistics: Flexera 2023 State of the Cloud Report. Flexera.* https://www.flexera.com/blog/finops/cloud-computing-trends-flexera-2023-state-of-the-cloud-report/
3. Khomchak, M. (2024). Enterprise private cloud platforms: A systematic review of key vendors. *International Journal of Wireless and Microwave Technologies, 14(4),* 1–14. https://doi.org/10.5815/ijwmt.2024.04.01
4. Mell, P., & Grance, T. (2011). The NIST definition of cloud computing. *National Institute of Standards and Technology, 53(6),* 50.
5. Al-Otaibi, S. Z. (2022). Data Security Challenges and Solutions in Cloud Computing: Critical Review. *Communications in Mathematics and Applications, 13(2),* 795.
6. Nassif, A. B., Talib, M. A., Nasir, Q., Albadani, H., & Dakalbab, F. M. (2021). Machine learning for cloud security: a systematic review. *IEEE Access, 9,* 20717–20735.
7. Süß, F., Freimuth, M., Aßmuth, A., Weir, G. R., & Duncan, B. (2024). *Cloud security and security challenges revisited.* arXiv preprint arXiv:2405.11350.
8. Vaka, P. R. (n.d.). *Cloud Security: Challenges, Methodologies, And Future Directions*.
9. Makulov, K., Chikrii, À., Lakhno, V., Yagaliyeva, B., Malyukov, V., Malyukova, I. N. N. A., & Lakhno, M. (2025). Cloud Platform Selection Model in the Framework of Differential Quality Game with Fuzzy Information. *IEEE Access*.
10. Cayirci, E., Garaga, A., Santana de Oliveira, A., & Roudier, Y. (2016). A risk assessment model for selecting cloud service providers. *Journal of Cloud Computing, 5(1),* 14.
11. Pape, S., Paci, F., Jürjens, J., & Massacci, F. (2020). Selecting a Secure Cloud Provider—An Empirical Study and Multi Criteria Approach. *Information, 11(5),* 261.

12. Da Silva, C. A., Ferreira, A. S., & de Geus, P. L. (2012). A methodology for management of cloud computing using security criteria. *2012 IEEE Latin America Conference on Cloud Computing and Communications (LatinCloud)*, 49–54. https://doi.org/10.1109/LatinCloud.2012.6508157
13. Khomchak, M. (2024). A Comprehensive Taxonomy of Modern Public Cloud Services for Infrastructure Selection. *International Journal of Computing, 23(3)*, 468–475. https://doi.org/10.47839/ijc.23.3.3667
14. *National vulnerability database (NVD).* (2025). NIST. https://www.nist.gov/programs-projects/national-vulnerability-database-nvd
15. *National vulnerability database (NVD).* (2025). NIST. https://www.nist.gov/programs-projects/national-vulnerability-database-nvd
16. *Vulnerability metrics: CVSS. National Vulnerability Database*. (n.d.). National Institute of Standards and Technology. https://nvd.nist.gov/vuln-metrics/cvss