Аналіз методів проведення аудиту безпеки хмарного середовища відповідно до міжнародних стандартів

Analysis of Methods for Conducting Cloud Security Audits According to International Standards

Владислав Франкевич [A]
студент кафедри Захист інформації, e-mail: vladyslav.frankevych.kb.2021@lpnu.ua, ORCID0009-0006-7888-3861

Соломія Долішня [A]
студент кафедри Захист інформації, e-mail: solomiia.dolishnia.kb.2021@lpnu.ua, ORCID: 0009-0002-2038-4374

Вікторія Савчук [A]
студент кафедри Захист інформації, e-mail: viktoriia.savchuk.kb.2021@lpnu.ua, ORCID: 0009-0003-3904-7391

Євгеній Курій [A]
асистент кафедри Захист інформації, e-mail: yevhenii.o.kurii@lpnu.ua, ORCID: 0000-0002-3423-5655

Віталій Сусукайло [A]
Corresponding author: доктор філософії, асистент кафедри Захисту інформації, e-mail: vitalii.a.susukailo@lpnu.ua, ORCID: 0000-0003-4431-9964

Vladyslav Frankevych [A]
Student of the Department Information Protection, e-mail: vladyslav.frankevych.kb.2021@lpnu.ua, ORCID0009-0006-7888-3861

Solomiia Dolishnia [A]
Student of the Department Information Protection, e-mail: solomiia.dolishnia.kb.2021@lpnu.ua, ORCID: 0009-0002-2038-4374

Viktoriia Savchuk [A]
Student of the Department Information Protection, e-mail: viktoriia.savchuk.kb.2021@lpnu.ua, ORCID: 0009-0003-3904-7391

Yevhenii Kurii [A]
Assistant of the Department, e-mail: yevhenii.o.kurii@lpnu.ua, ORCID: 0000-0002-3423-5655

Vitalii Susukailo [A]
Corresponding author: Doctor of Philosophy, Assistant of the Department, e-mail: vitalii.a.susukailo@lpnu.ua, ORCID: 0000-0003-4431-9964

[A] Національний університет "Львівська політехніка", Львів, Україна
[A] Lviv Polytechnic National University, Lviv, Ukraine

Received: April 8, 2025 | Revised: April 28, 2025 | Accepted: April 30, 2025

DOI: 10.33445/sds.2025.15.2.19

Мета роботи: Порівняння методів аудиту безпеки хмарних середовищ (ручний, автоматизований, вбудований) для визначення їх ефективності у відповідності міжнародним стандартам, зокрема, з урахуванням специфіки хмарних платформ та мінімізацією ризиків.

Метод дослідження: Емпіричне дослідження.

Результати дослідження: Автоматизовані інструменти забезпечують швидкість та економічність, однак ручний аудит, попри свою трудомісткість, забезпечує глибину аналізу нестандартних конфігурацій. Вбудовані засоби надають миттєвий огляд безпеки, але мають обмежену гнучкість, тоді як інтеграція стандартів, хоча й підвищує загальний рівень захищеності, виявляє прогалини в адаптації вимог до специфічних потреб організацій.

Теоретична цінність дослідження: Дослідження підтверджує актуальність існуючих теоретичних рамок, а саме міжнародних стандартів для оцінки безпеки, але вказує на необхідність їх адаптації до динамічних хмарних середовищ. Результати підкреслюють роль адаптивних моделей для покращення відповідності стандартам.

Практична цінність дослідження: Системні адміністратори та інженери з безпеки можуть комбінувати автоматизовані інструменти, ручний аудит та вбудовані засоби для оптимізації витрат і підвищення точності оцінки безпеки. Інтеграція машинного навчання для прогнозування ризиків і адаптації стандартів дозволить розробляти проактивні стратегії захисту хмарних середовищ, зокрема для фільтрації хибнопозитивних результатів та пріоритизації вразливостей.

Цінність дослідження: Порівняльний аналіз трьох методів з урахуванням їх взаємодії, вартості та відповідності стандартам. Надано практичні критерії для вибору стратегій безпеки за обмежених ресурсів.

Тип статті: Емпіричне дослідження з елементами теоретичного аналізу.

Purpose: Comparison of cloud security audit methods (manual, automated, embedded) to determine their effectiveness in accordance with international standards, in particular, taking into account the specifics of cloud platforms and risk minimization.

Method: The empirical study.

Findings: Automated tools provide speed and cost-effectiveness, but manual auditing, while laborious, reveals the depth of analysis of non-standard configurations. Built-in tools provide an instant security overview but have limited flexibility, while standards integration, while increasing the overall level of security, reveals gaps in adapting requirements to the specific needs of organizations.

Theoretical implications: The study confirms the relevance of existing theoretical frameworks, namely international standards for security assessment, but points to the need to adapt them to dynamic cloud environments. The results highlight the role of adaptive models in improving compliance with standards.

Practical implications: System administrators and security engineers can combine automated tools, manual auditing, and built-in tools to optimize costs and improve the accuracy of security assessments. Integrating machine learning for risk prediction and standards adaptation will allow for proactive cloud security strategies, including filtering false positives and prioritizing vulnerabilities.

Value: A comparative analysis of three methods, taking into account their interaction, cost, and compliance with standards. Practical criteria for choosing security strategies under limited resources are provided.

Paper type: Empirical research with elements of theoretical analysis.

Ключові слова: інформаційна безпека; хмарна безпека; аудит безпеки; міжнародні стандарти безпеки; автоматизований аудит.

Key words: information security; cloud security; security audit; international security standards; automated audit.

Вступ

Сучасні хмарні середовища, такі як Microsoft 365, Amazon Web Services та Google Workspace, стали основою цифрової інфраструктури для більшості організацій, що працюють у різноманітних галузях. Проте зростаючі кіберзагрози, складність конфігурацій цих платформ та вимоги до відповідності міжнародним стандартам безпеки, таким як ISO 27001, SOC 2, NIST CSF, створюють серйозні виклики для забезпечення належного рівня захищеності. У цих умовах питання безпеки стає критично важливим, адже навіть найменші вразливості можуть призвести до значних фінансових та репутаційних втрат для організацій.

Для оцінки рівня безпеки хмарних середовищ використовуються різні підходи, зокрема автоматизовані та вбудовані інструменти, які мають на меті забезпечити швидкість і ефективність аудиту. Проте такі інструменти часто стикаються з обмеженнями щодо підтримки специфічних фреймворків і вимог. Ручні методи аудиту, хоча і дають змогу здійснити глибокий аналіз нестандартних налаштувань, є трудомісткими і не завжди відповідають сучасним вимогам ефективності.

Метою даної роботи є вивчення та порівняння різних підходів до аудиту безпеки хмарних середовищ, визначення їхніх переваг і недоліків, а також оцінка їх ефективності в контексті міжнародних стандартів безпеки.

Теоретичні основи дослідження

Хмарні середовища забезпечують доступ до обчислювальних ресурсів через інтернет, що надає організаціям гнучкість, масштабованість та економічну ефективність. Вони характеризуються можливістю швидко змінювати обсяги ресурсів (масштабування вгору або вниз), автоматично адаптуватися до навантаження та надавати доступ до даних у будь-який час і з будь-якого місця. Модель оплати “pay-as-you-go” дозволяє знижувати витрати на підтримку інфраструктури, а централізоване управління спрощує контроль над ресурсами. Реплікація даних та інтеграція з різними платформами забезпечують високу доступність та адаптивність. Однак ці переваги створюють виклики для безпеки, особливо через конфігураційні помилки та несанкціонований доступ.

Хмарні сервіси класифікуються за рівнем наданих ресурсів: IaaS, PaaS та SaaS. IaaS надає базову інфраструктуру (наприклад, AWS EC2, Azure VMs), що дозволяє користувачам контролювати ресурси, але потребує технічної експертизи та відповідальності за безпеку. PaaS (Google App Engine, Heroku) спрощує розробку додатків, однак зменшує контроль над інфраструктурою. SaaS (Microsoft 365, Salesforce) надає готові програмні рішення, які не потребують установки, але обмежують можливості кастомізації.

Критичні ресурси включають дані (персональні, фінансові, конфіденційні), обчислювальні ресурси (сервери, бази даних), мережеву інфраструктуру (брандмауери, VPN) та інструменти управління (системи аутентифікації, API). Наприклад, в AWS важливими є IAM, S3-бакети та KMS, у Microsoft Azure — AAD, Blob Storage та Security Center. Компрометація цих ресурсів може призвести до фінансових збитків, порушення безперервності бізнесу або втрати довіри клієнтів.

Основні вектори атак у хмарних середовищах включають неправильну конфігурацію, таку як відкриті S3-бакети та некоректні політики доступу, а також вразливості програмного забезпечення, як-от непатчені програми чи контейнери. До того ж, фішинг та компрометація облікових записів, зокрема через брутфорс-атаки або викрадені токени, є поширеними методами доступу до систем. Атаки типу DoS/DDoS можуть призвести до недоступності сервісів, що серйозно порушує роботу організацій. Інсайдерські загрози також становлять небезпеку, коли співробітники здійснюють зловмисні дії. Серед найбільших загроз у хмарних середовищах можна виділити втрату даних, компрометацію конфіденційності, фінансові

збитки через несанкціоноване використання ресурсів та репутаційні втрати через витоки інформації.

Основні загрози в хмарних середовищах створюють серйозні виклики для організацій, які використовують такі сервіси. Неправильна конфігурація, вразливості програмного забезпечення, компрометація облікових записів, DoS/DDoS-атаки та інсайдерські загрози можуть спричинити фінансові збитки, порушення безперервності бізнесу та втрату довіри клієнтів. Успішна експлуатація цих загроз може призвести до витоку даних, несанкціонованого використання ресурсів та порушення роботи критичних сервісів. Для зменшення цих ризиків необхідно застосовувати ефективні заходи безпеки та методи управління ризиками.

Ефективність управління ризиками в хмарних середовищах безпосередньо залежить від належної реалізації контролів безпеки, зокрема рекомендацій CIS Benchmarks. Для оцінки ризиків використовується модель, яка враховує ймовірність виникнення інциденту (P) та його потенційні втрати (L). Ризик (R) визначається за формулою $R = P \cdot L$, де P — ймовірність виникнення події. L — потенційні втрати, що виникають внаслідок інциденту.

Аналіз ризикових сценаріїв допомагає виявити найбільш ймовірні загрози для безпеки в хмарі. Один із таких сценаріїв — відкритий S3 Bucket з конфіденційною інформацією. Якщо не налаштувати політику "Block public access" для S3-бакетів, це створює ризик несанкціонованого доступу до даних. За оцінками, до 30% хмарних середовищ можуть містити такі помилки, що дає ймовірність виникнення інциденту на рівні 30%. У разі компрометації може відбутися витік персональних даних клієнтів. Якщо припустити, що в системі знаходиться 10000 записів, а середня вартість одного запису згідно з даними IBM на 2023 рік складає 165 доларів (6876 грн) [1], то загальна сума потенційних втрат становитиме 68760000 грн. Враховуючи ймовірність виникнення інциденту на рівні 30%, ризик для організації буде становити 20628000 грн.

Захист інформації та забезпечення безпеки хмарних середовищ є критично важливим аспектом сучасної кібербезпеки. Міжнародні стандарти безпеки встановлюють загальні вимоги та кращі практики для захисту даних, інфраструктури та забезпечення належної безпеки хмарних сервісів.

ISO/IEC 27001 є міжнародним стандартом для систем управління інформаційною безпекою (ISMS), який визначає вимоги щодо створення, реалізації, підтримки та вдосконалення системи управління інформаційною безпекою на підприємстві. Згідно з цим стандартом, організації повинні проводити оцінку ризиків для своїх інформаційних активів і вживати відповідні заходи для їх мінімізації, а також налаштовувати системи та процеси для обмеження доступу до конфіденційної інформації [2]. Також важливим є регулярний моніторинг діяльності та проведення аудитів, щоб виявити потенційні вразливості в інформаційних системах. Стандарт передбачає наявність процедур для оперативного реагування на інциденти безпеки та встановлює вимоги до оцінки та контролю безпеки постачальників і партнерів, що мають доступ до інформаційних систем.

SOC 2 (System and Organization Controls 2) — це набір стандартів, що визначають вимоги до систем обробки даних та встановлюють критерії для перевірки безпеки, доступності, конфіденційності, цілісності обробки та конфіденційності даних. Цей стандарт є важливим для компаній, які працюють з персональними даними, особливо для хмарних провайдерів. SOC 2 оцінює, чи захищена система від несанкціонованого доступу, чи здатна вона бути доступною і готовою до використання, чи забезпечується точність та якість обробки даних, а також чи надається належний захист конфіденційної інформації, що обробляється або зберігається в системах. Крім того, особливу увагу приділяється контролю доступу до персональних і корпоративних даних, що є важливою частиною забезпечення їх безпеки та конфіденційності.

GDPR (General Data Protection Regulation) є законодавчим актом Європейського Союзу, який регулює обробку персональних даних і є обов’язковим для організацій, що обробляють

дані громадян ЄС, незалежно від їхнього місцезнаходження [3]. Однією з основних вимог для хмарних середовищ є забезпечення прозорості та контролю, що означає право користувачів знати, які дані збираються та як вони обробляються. Крім того, організації повинні отримати явну згоду користувачів перед обробкою їх персональних даних, надавши їм право на доступ до своїх даних та можливість вимагати їх виправлення. Окрім цього, хмарні сервіси зобов'язані забезпечити належний рівень безпеки обробки персональних даних, а також негайно, протягом 72 годин, повідомляти про будь-які порушення безпеки даних.

NIST CSF (Cybersecurity Framework) — це набір керівних принципів, розроблений Національним інститутом стандартів і технологій США для покращення кібербезпеки в організаціях. Він визначає вимоги, що забезпечують захист хмарних середовищ через три основні функції: ідентифікацію ризиків, захист систем та даних, а також виявлення потенційних загроз. Це включає в себе оцінку ризиків, встановлення засобів для захисту інфраструктури та постійний моніторинг на наявність загроз. Крім того, NIST CSF передбачає розробку планів реагування на інциденти безпеки та відновлення систем після можливих кіберінцидентів.

CIS Controls v8 — це набір з 18 контролів, що визначають найкращі практики для забезпечення кібербезпеки організацій [4]. Вони спрямовані на правильний захист хмарних середовищ, включаючи ідентифікацію та управління активами, що включає визначення всіх пристроїв, програм і даних, що зберігаються в хмарі, управління вразливостями через регулярне сканування та патчинг, а також захист даних за допомогою шифрування на етапах зберігання і передачі. Окрім того, важливим є управління доступом із застосуванням принципу найменших привілеїв і багатоетапної автентифікації для контролю доступу, а також моніторинг та реагування на інциденти, що включає виявлення аномалій і негайну реакцію на інциденти безпеки.

Використання бенчмарків та фреймворків для підвищення безпеки хмарних середовищ є важливим кроком для забезпечення конфіденційності, цілісності та доступності даних. Ці стандарти надають рекомендації з налаштувань конфігурацій, які допомагають захистити хмарні інфраструктури від різноманітних кіберзагроз. Вони включають практичні керівництва, які розроблені з урахуванням найкращих практик в індустрії, та допомагають організаціям забезпечити належний рівень безпеки для своїх хмарних середовищ.

CIS Benchmarks (Center for Internet Security Benchmarks) — це набір рекомендованих конфігурацій для більш ніж 25 продуктів різних постачальників [5]. Вони розроблені експертами з кібербезпеки по всьому світу з метою забезпечення кращого захисту від загроз та вразливостей для інформаційних систем. CIS Benchmarks складаються з конкретних рекомендацій щодо налаштування безпеки, які можуть бути застосовані для широкого спектра хмарних платформ та інших технологій.

До хмарних постачальників, для яких існують CIS Benchmarks, належать Alibaba Cloud, Amazon Web Services (AWS), Google Cloud Computing Platform (GCP), Google Workspace, IBM Cloud Foundations, Microsoft 365, Microsoft Azure, Microsoft Dynamics 365 Power Platform, Oracle Cloud Infrastructure.

CIS Benchmarks забезпечують організації конкретними кроками для посилення безпеки їхніх хмарних середовищ, включаючи налаштування доступу, шифрування даних, моніторинг безпеки та методи реагування на інциденти. Використання CIS Benchmarks дозволяє мінімізувати ризики внаслідок людських помилок або невідповідності стандартам безпеки.

CISA — це агентство Міністерства внутрішньої безпеки США, яке відповідає за забезпечення кібербезпеки та захист критичної інфраструктури [6]. CISA керує національними програмами з кібербезпеки та надає ресурси для організацій, що працюють із критично важливою інформацією, зокрема в хмарних середовищах [7]. Одним із важливих проектів агентства є Secure Cloud Business Applications (SCuBA).

Проект SCuBA надає рекомендації та інструменти для захисту хмарних бізнес-додатків і забезпечує захист федеральних даних, що зберігаються в хмарі [8]. SCuBA фокусується на забезпеченні безпеки для інформаційних активів у хмарних середовищах через стандартизовані, сучасні та керовані конфігурації безпеки. Це дозволяє ефективно налаштовувати безпеку хмарних додатків і забезпечити конфіденційність даних.

SCuBA включає важливі фреймворки для забезпечення безпеки в хмарних середовищах, такі як Microsoft 365 (M365) і Google Workspace (GWS). Для обох платформ існують спеціалізовані Secure Configuration Baselines, що надають прості та зрозумілі рекомендації для налаштування безпеки. Ці базові конфігурації сприяють підвищенню безпеки хмарних сервісів, узгоджуючи налаштування з унікальними вимогами і рівнями ризику кожної організації.

Бенчмарки та фреймворки, такі як CIS Benchmarks та CISA спеціалізовані базові конфігурації безпеки, є важливими інструментами для підвищення безпеки хмарних середовищ. Вони надають чіткі, погоджені рекомендації для налаштування хмарних систем і допомагають організаціям захистити свої дані від потенційних загроз. Інтеграція цих стандартів у практики забезпечення безпеки допомагає підвищити рівень захисту та зменшити ймовірність виникнення інцидентів безпеки.

Ручне проведення аудиту безпеки хмарного середовища полягає в аудиті конфігураційних налаштувань сервісів, що працюють у хмарі, з метою перевірки їх відповідності стандартам безпеки, таким як CIS Benchmarks, CISA Baselines чи іншим рекомендаціям щодо підвищення безпеки. На початковому етапі необхідно визначити хмарне середовище та відповідні сервіси, які підлягають перевірці, а також встановити стандарти для перевірки, які будуть використовуватись для оцінки безпеки.

Далі аудитор безпосередньо входить у консоль керування хмарним середовищем і перевіряє налаштування різних сервісів. Він аналізує налаштування доступу, конфігурації безпеки, параметри логів та моніторингу, налаштування резервного копіювання і відновлення даних, а також політики безпеки для інтегрованих програм і сервісів. Після цього результати перевірки порівнюються з вимогами стандартів, що дозволяє оцінити відповідність налаштувань хмарних сервісів встановленим критеріям безпеки і виявити потенційні вразливості.

Проведення аудиту супроводжується складанням детального звіту, в якому фіксуються всі виявлені невідповідності стандартам безпеки. У звіті надається перелік знайдених проблем, оцінка ризиків для організації та рекомендації щодо виправлення недоліків, при цьому зазначаються конкретні вимоги фреймворків або бенчмарків, які не виконуються.

Ручне проведення аудиту має значні переваги, серед яких можливість глибокого аналізу конкретних аспектів налаштувань, що можуть бути пропущені автоматизованими інструментами. Аудитор може перевірити нестандартні конфігурації, детально проаналізувати кожне налаштування та виявити навіть найменші порушення, що дозволяє забезпечити більш високу точність перевірки. Також ручне проведення аудиту дозволяє охопити більший обсяг аспектів безпеки, ніж це може зробити автоматизована перевірка, оскільки аудитор має змогу врахувати додаткові моменти, які не входять до базових вимог стандартних фреймворків.

Однак цей метод має і недоліки. Проведення аудиту вручну потребує значно більше часу порівняно з автоматизованими рішеннями, особливо в умовах великих або складних хмарних інфраструктур. Також існує ризик помилок через людський фактор, коли аудитор може пропустити важливі налаштування або неправильно їх інтерпретувати. Цей підхід не завжди ефективний для масштабних проектів, оскільки перевірка великої кількості ресурсів може призвести до значного ускладнення процесу і збільшення вартості робіт. Крім того, складання звіту вручну є трудомістким етапом, що підвищує ризик помилок та пропусків.

Ручне проведення аудиту залежить від досвіду аудитора, тому відсутність кваліфікованих спеціалістів може знизити якість перевірки і уповільнити весь процес.

Автоматизовані засоби проведення аудиту безпеки хмарних середовищ, зокрема скрипти та інструменти, як-от Prowler, дозволяють значно підвищити ефективність процесу. Вони охоплюють різноманітні стандарти, фреймворки та бенчмарки, що зменшує час проведення аудиту та забезпечує більш об'єктивну оцінку стану безпеки. Prowler є потужним відкритим інструментом для оцінки безпеки, який підтримує хмарні платформи, такі як AWS, Azure, GCP та Kubernetes, і дозволяє здійснювати безперервний моніторинг, оцінки безпеки, аудити, відповіді на інциденти, забезпечення відповідності стандартам, зміцнення захисту та готовність до проведення судово-розслідувальних заходів [9].

Інструмент охоплює понад 500 перевірок для різних хмарних платформ, включаючи стандарти CIS, NIST 800, FedRAMP, PCI-DSS, GDPR, SOC2 та інші. Завдяки автоматизації процесу, Prowler дозволяє значно зменшити час, необхідний для оцінки конфігурацій, а також знижує ризики, пов'язані з людським фактором. Детальні звіти, що генеруються інструментом, дозволяють оперативно оцінити відповідність хмарного середовища вимогам безпеки, а також отримувати історичні дані для аналізу тенденцій у безпеці (рис. 1).

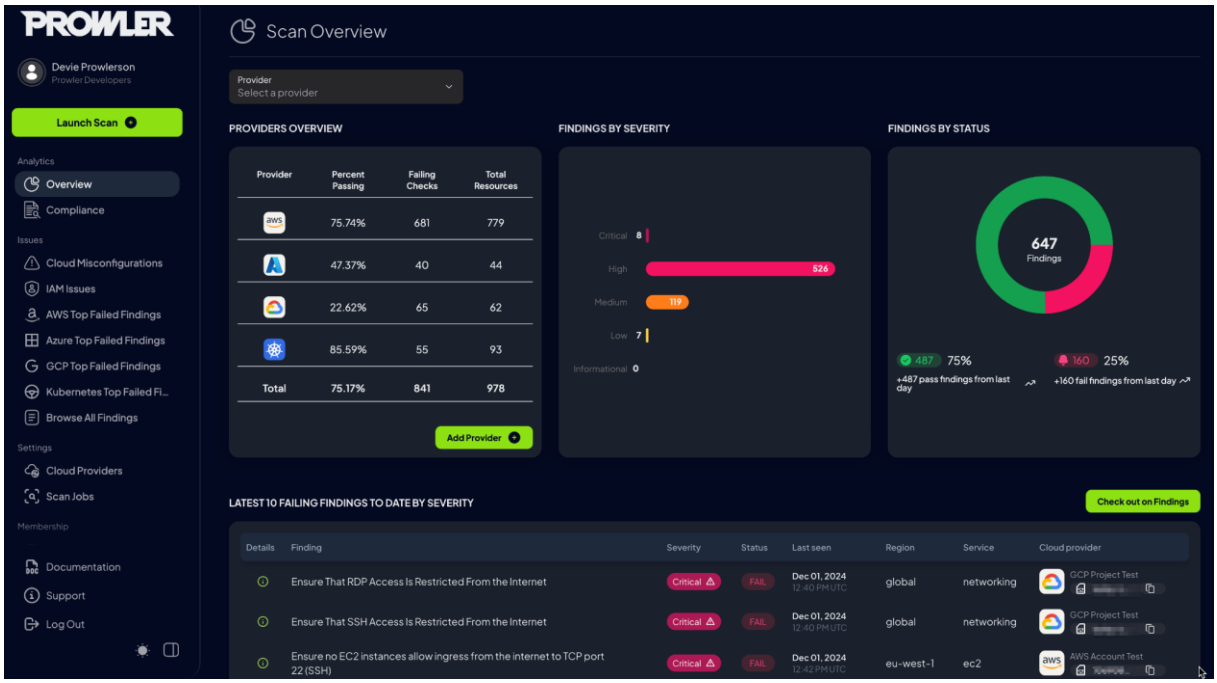

Рисунок 1 – Інтерфейс веб-додатку Prowler
Джерело: https://docs.prowler.com/projects/prowler-open-source/en/latest/

Автоматизація проведення аудиту значно скорочує час перевірки безпеки, оскільки інструмент здатний здійснювати перевірки в кілька разів швидше за ручний метод, що дозволяє оперативно виявляти вразливості та недоліки. Генеровані звіти, які базуються на заданих стандартах та фреймворках, дають змогу отримати чітку та зрозумілу оцінку стану безпеки, а також порівнювати результати з попередніми перевірками для відслідковування змін. Підтримка численних фреймворків та стандартів дозволяє проводити оцінку відповідності хмарних середовищ міжнародним вимогам, а інтеграція з різноманітними системами аналітики забезпечує глибокий аналіз стану безпеки, надаючи детальну інформацію про потенційні загрози, тренди та патерни.

Незважаючи на переваги, Prowler має свої обмеження. Не всі хмарні провайдери можуть бути повністю охоплені необхідними перевірками, що стає проблемою для менш

популярних платформ або специфічних стандартів [10]. Налаштування інструменту на власній інфраструктурі може бути трудомістким процесом для користувачів без відповідного досвіду, а також оцінка конфігурацій без врахування специфіки конкретних даних чи критичності ресурсів може призводити до недооцінки деяких проблем. Крім того, можливості кастомізації звітів зазвичай обмежені у порівнянні з ручними звітами, які дозволяють створити більш індивідуалізовану інформацію з урахуванням конкретних вимог організації.

ScubaGear є інструментом для оцінки безпеки, частиною проекту SCuBA, розробленого Агентством з кібербезпеки та інфраструктурної безпеки США (CISA). Він призначений для перевірки конфігурацій Microsoft 365 на відповідність політикам безпеки, описаним у документах Microsoft 365 Secure Configuration Baselines, що дозволяє адміністраторам перевіряти свої середовища для забезпечення захисту інформації, що створюється, зберігається та передається через хмарні бізнес-застосунки. ScubaGear працює за трьома етапами (рис. 2): спочатку здійснюється запит через PowerShell до API Microsoft 365 для отримання налаштувань, потім ці налаштування порівнюються з політиками безпеки за допомогою Open Policy Agent, а в кінцевому результаті формується звіт про результати порівняння, який може бути наданий у форматах HTML, JSON або CSV.

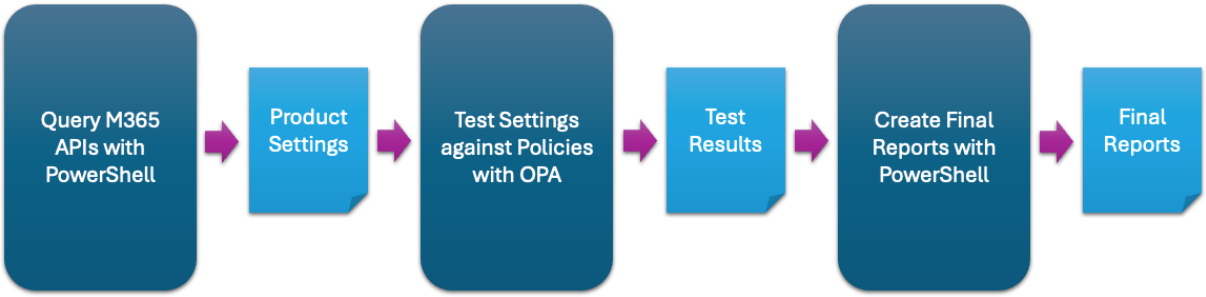

Рисунок 2 – Етапи роботи ScubaGear
Джерело: https://github.com/cisagov/ScubaGear

Інструмент може працювати як в інтерактивному режимі, коли через термінал відкривається веб-вікно для надання доступу до акаунту Microsoft, так і в безінтерактивному режимі, коли налаштовується службовий принципал з відповідними дозволами. Налаштування для безінтерактивного запуску включає створення службового принципала, формування сертифіката та його зв'язування з принципалом. Використання ScubaGear дозволяє автоматизувати перевірки конфігурацій Microsoft 365, що знижує навантаження на адміністраторів і прискорює процес перевірки, хоча налаштування службового принципала може бути складним для пересічного користувача. Інструмент орієнтований виключно на Microsoft 365, що обмежує його застосування в інших хмарних середовищах, а можливості кастомізації перевірок і звітів залишаються обмеженими, особливо при тестуванні нестандартних налаштувань або застосуванні специфічних внутрішніх політик безпеки.

ScubaGoggles є інструментом для оцінки безпеки, розробленим у рамках проекту SCuBA агентством CISA, і призначеним для перевірки конфігурацій Google Workspace на відповідність політикам безпеки, описаним у документах SCuBA Secure Configuration Baseline. Як аналог для Google Workspace, цей інструмент допомагає адміністраторам перевірити налаштування своїх середовищ для забезпечення захисту інформації, яка створюється, зберігається та передається через хмарні бізнес-застосунки Google. ScubaGoggles використовує трьохетапний процес: спочатку здійснюється експорт налаштувань за допомогою Google Admin SDK API, дані серіалізуються у формат JSON і доповнюються метаданими організації, після чого отримані налаштування порівнюються з вимогами, прописаними в SCuBA Secure Configuration Baseline за допомогою OPA Rego, і нарешті формується звіт у форматах HTML та JSON [11]. Основна

частина перевірок залежить від журналів адміністратора Google Workspace, тому при відсутності певного журналу інструмент повідомляє про необхідність вручну перевірити відповідну конфігурацію.

Для роботи ScubaGoggles необхідно завантажити інструмент та встановити залежності, включаючи Python та OPA Executable, а також налаштувати методи аутентифікації, такі як OAuth або службовий обліковий запис для автоматизованих процесів, і використати конфігураційний файл для визначення параметрів аудиту. Використання цього інструменту дозволяє автоматизувати перевірку конфігурацій Google Workspace відповідно до актуальних стандартів, що значно прискорює процес порівняння і забезпечує консистентність перевірок, а зручна генерація звітів у форматах HTML та JSON дозволяє легко інтегрувати результати в існуючі процеси безпеки компанії. Проте ScubaGoggles перебуває на стадії альфа-версії, тому існує ризик виникнення помилок або некоректних результатів перевірок, а також можливе обмеження перевірки деяких політик через відсутність відповідних журналів у Google Workspace. Обмежена можливість кастомізації перевірок та необхідність налаштування сертифікатів і прав доступу до акаунтів може ускладнити використання інструменту для адміністраторів без належного досвіду.

Amazon Web Services (AWS) пропонує потужні вбудовані інструменти для забезпечення безпеки в хмарному середовищі, серед яких IAM Trusted Advisor, IAM Access Analyzer та AWS Security Hub. Ці засоби автоматизують процеси проведення аудиту та моніторингу безпеки, дозволяючи організаціям швидко виявляти вразливості та відповідати на них [12]. AWS Security Hub виступає як центр управління безпекою, що дозволяє автоматизувати перевірку безпеки, отримувати попередження про потенційні загрози та порушення, а також отримувати огляд загального стану безпеки для всіх акаунтів AWS. Він централізує перевірки та попередження безпеки від різних сервісів AWS і підтримуваних сторонніх продуктів, що спрощує процес моніторингу та реагування. Крім того, завдяки інтеграції з іншими сервісами, такими як EventBridge та AWS Config, Security Hub може автоматично оновлювати статуси виявлених проблем, дозволяючи організаціям ефективно керувати ризиками. Водночас, використання цього інструменту пов’язане з певними витратами, оскільки оплата визначається за кількістю перевірок, подій та автоматизованих правил, а для ефективної роботи потрібно забезпечити належну інтеграцію з іншими сервісами AWS [13].

AWS Trusted Advisor допомагає оптимізувати інфраструктуру, знижувати витрати та покращувати безпеку шляхом надання рекомендацій щодо покращення конфігурацій ресурсів. Він виявляє потенційні вразливості, зокрема неправильні налаштування доступу або надмірно широкі дозволи, а також пропонує рекомендації щодо оптимізації витрат за рахунок видалення неактивних ресурсів. Проте повний доступ до всіх його функцій можливий лише з підпискою на Business або Enterprise Support, що може стати додатковим фінансовим навантаженням.

AWS IAM Access Analyzer спрямований на моніторинг та аналіз доступу до ресурсів AWS, допомагаючи визначити, хто має доступ до критичних даних і чи не надано надмірних дозволів зовнішнім користувачам. Цей інструмент аналізує політики доступу і забезпечує автоматичне сповіщення про будь-які зміни, що є важливим для оперативного реагування на потенційні загрози. Однак для отримання повної інформації про доступ може знадобитися додаткове налаштування або інтеграція з іншими сервісами, такими як AWS CloudTrail, що може ускладнити процес.

Microsoft 365 також пропонує потужні інструменти для аудиту безпеки, серед яких Microsoft Secure Score та Microsoft Purview Compliance Manager. Microsoft Secure Score дозволяє організаціям оцінити рівень їхньої безпеки шляхом вимірювання виконання рекомендованих заходів, що відображається у вигляді числового показника, який порівнюється із середніми значеннями для подібних організацій. Цей інструмент дає

можливість аналізувати поточний стан безпеки, відстежувати виконання ключових показників ефективності та визначати напрямки для покращення [14]. Microsoft Purview Compliance Manager, у свою чергу, допомагає організаціям автоматично оцінювати відповідність вимогам стандартів та регламентів, пропонуючи детальні кроки для покращення відповідності та зниження ризиків, пов'язаних із захистом даних. Разом ці інструменти створюють комплексну систему для управління безпекою та відповідністю у середовищі Microsoft 365 [15].

Google Workspace надає адміністраторам можливість моніторити та налаштовувати параметри захисту через спеціально розроблений розділ Security Health, доступний в консолі адміністратора. Цей інструмент забезпечує зручний огляд налаштувань безпеки організації, дозволяючи відстежувати стан двофакторної аутентифікації, управління доступом до Google Drive, безпечну обробку електронної пошти та керування мобільними пристроями. Сторінка безпеки дає змогу визначати конфігурації, які можуть становити ризик, і отримувати рекомендації для їх усунення, враховуючи як потреби безпеки, так і специфіку роботи організації. Адміністратори можуть моніторити налаштування в розрізі організаційних підрозділів, змінювати параметри для дочірніх одиниць та враховувати особливості тарифних планів, що впливають на функціонал інструмента. Цей підхід дозволяє забезпечити безперебійну та безпечну роботу організації в умовах постійно змінюваних викликів у кіберпросторі.

Постановка проблеми

Основною проблемою, розглянутою в цій статті, є відсутність універсальних методів аудиту, які поєднують швидкість, глибину аналізу та постійний моніторинг, відповідаючи вимогам міжнародних стандартів. Автоматизовані інструменти здатні швидко виявляти вразливості, але не здатні адаптуватися до нестандартних налаштувань систем. З іншого боку, ручний аудит є надзвичайно трудомістким і дорогим.

У таких умовах виникає необхідність у розробці системного підходу, який враховує ці обмеження і дозволяє забезпечити ефективний аудит. Ігнорування цієї проблеми може призвести до значних труднощів у підтримці безпеки та стабільності інформаційних систем, особливо в умовах постійного зростання кіберзагроз і складності технологічних середовищ.

Попри важливість цієї теми, в науковій літературі спостерігається недостатня увага до створення інтегрованих методів аудиту, які можуть задовольнити сучасні вимоги до швидкості, точності та адаптивності. Рішення цієї проблеми потребує комплексного підходу, що дозволить забезпечити ефективний моніторинг та виявлення вразливостей в умовах постійно змінюваних технологічних умов.

Методологія дослідження

У цьому дослідженні було обрано хмарне середовище Microsoft 365 як об'єкт аудиту безпеки через його популярність, широке використання в корпоративних середовищах і наявність базових інструментів управління безпекою, що дозволяють аналізувати й оцінювати рівень захисту даних. Дослідження проводилось на тестовому обліковому записі з безкоштовним пробним періодом, при якому створено мінімалістичне середовище, що імітує роботу невеликої організації, з мінімально необхідними ресурсами. У цьому середовищі реалізовано два типи користувачів: адміністратор із повним доступом для управління ресурсами та звичайний користувач із обмеженим доступом до корпоративних даних у OneDrive і поштових скриньках Exchange Online. Усі файли в OneDrive за замовчуванням є приватними, а для адміністратора ввімкнено багатофакторну автентифікацію (MFA). Така конфігурація дозволяє знизити складність дослідження, зберігаючи можливість детального аналізу налаштувань безпеки.

Критеріями оцінки безпеки було встановлено виявлення вразливостей у конфігурації хмарного середовища, оцінка ефективності наявних заходів безпеки та перевірка відповідності налаштувань загальноприйнятим рекомендаціям, таким як CIS Benchmarks. До основних показників належить аналіз налаштувань доступу до сховищ OneDrive та сайтів SharePoint, перевірка правильного розмежування прав доступу до публічних і приватних ресурсів, оцінка впровадження багатофакторної автентифікації, аналіз політик щодо паролів, моніторинг журналювання змін конфігурацій і доступу до об'єктів, порівняння конфігурації середовища з рекомендованими стандартами та виявлення слабких місць, що дозволяє оцінити потенційні ризики.

Ручне проведення аудиту налаштувань безпеки Microsoft 365 виконувалось за методикою, що базується на CIS Microsoft 365 Foundations Benchmark v3.1.0. Для автоматизованої оцінки стану безпеки та відповідності середовища Microsoft 365 було використано вбудоване рішення Compliance Manager з платформи Microsoft Purview. Для автоматизованого проведення аудиту також було використано сторонній сервіс ScubaGear, доступний з офіційного репозиторію GitHub [16]. Цей інструмент, що є частиною проекту SCuBA, розробленого Агентством з кібербезпеки та інфраструктурної безпеки США (CISA), перевіряє конфігурації Microsoft 365 на відповідність політикам безпеки, визначеним у Microsoft 365 Secure Configuration Baselines.

Результати

Дослідження показало, що безпека хмарних середовищ може перевірятися трьома підходами: ручним, автоматизованим та за допомогою вбудованих засобів. Для ручного проведення аудиту, що базується на стандартах CIS Benchmarks і CISA Baselines, середній час однієї перевірки складає 5 хвилин, що призводить до значних витрат часу при збільшенні кількості контролів. Автоматизовані засоби, такі як Prowler, ScubaGear та ScubaGoggles, дозволяють виконувати одну перевірку за 3 секунди, що суттєво скорочує загальний час аудиту навіть при великій кількості перевірок. Вбудовані засоби, як AWS Trusted Advisor, Security Hub, IAM Access Analyzer або Purview Manager, забезпечують збір даних у режимі реального часу, що дозволяє отримувати результати практично миттєво. Це порівняння підсумовано в табл. 1.

Таблиця 1 – Порівняння підходів проведення аудиту безпеки хмарних середовищ

Метод проведення аудиту	Засоби	Швидкість перевірки	Ресурси, необхідні для виконання	Ефективність у масштабах великої системи
Ручний	Немає	5 хвилин для кожної перевірки	Висока залежність від кваліфікації та досвіду аналітика	Низька, оскільки потребує набагато більше ресурсів
Автоматизований	Prowler, ScubaGear, ScubaGoggles	3 секунди на одну перевірку	Необхідне налаштування інструментів, регулярне оновлення	Висока, оскільки може обробляти сотні перевірок за лічені хвилини
Вбудований	AWS Trusted Advisor, Security Hub, IAM Access Analyzer, Purview Manager	0 секунд, оскільки дані завжди доступні, збираються в реальному часі	Мінімальні: інтегровано в хмарне середовище; доступ через консоль або API	Максимальна, оскільки повністю інтегроване рішення

Розглянемо середню кількість перевірок для організації, що складається з 100 контролів, і порівняємо ефективність їх виконання (рис. 3). Ручний метод займає найбільше часу, досягаючи 500 хвилин, що значно перевищує час, витрачений на автоматизовані та

вбудовані рішення, особливо при збільшенні кількості перевірок. Автоматизований підхід дозволяє значно скоротити час виконання до 5 хвилин, що робить його швидким навіть для великої кількості перевірок, хоча вимагає певної підготовки. Вбудоване рішення є найефективнішим, оскільки надає дані миттєво без додаткового часу на виконання та працює в режимі реального часу, не потребуючи ручного запуску.

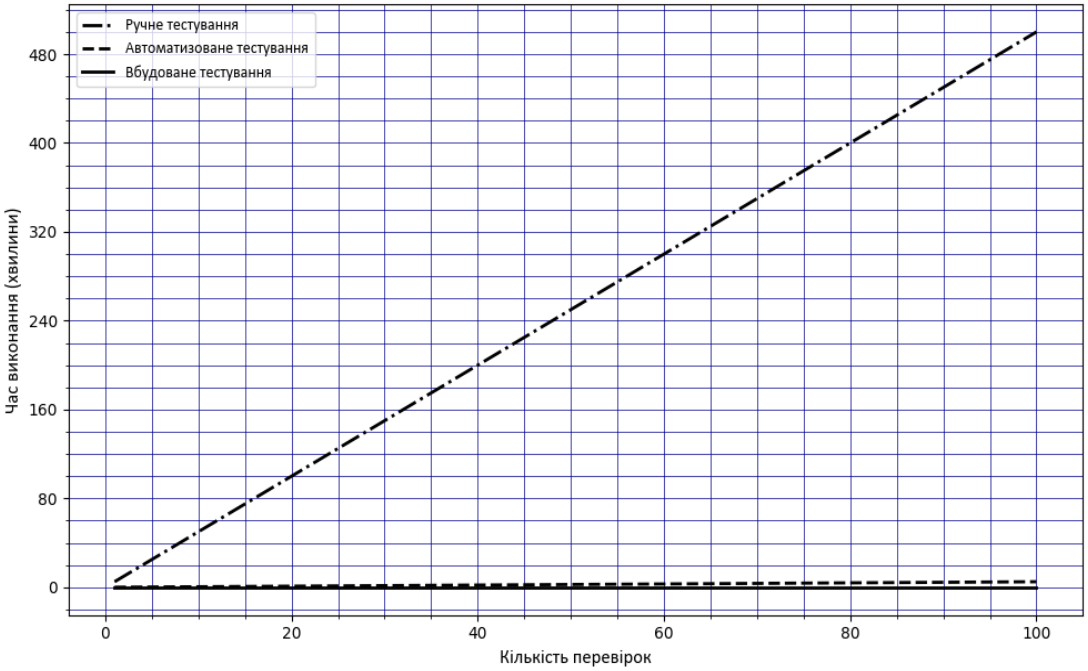

Рисунок 3 – Графік залежності часу від кількості перевірок

Ручний підхід забезпечує найвищий рівень деталізації завдяки можливості фахівця адаптувати перевірки, змінювати критичність контролів та враховувати специфіку організації, що дозволяє виявити навіть найменші невідповідності. Проте цей метод є трудомістким і залежить від кваліфікації спеціаліста. Автоматизовані засоби забезпечують стандартизовані звіти, які є корисними для загальної оцінки безпеки, але мають обмежені можливості для кастомізації, що може знижувати релевантність результатів для унікальних сценаріїв. Вбудовані засоби, такі як дашборди Microsoft Secure Score або AWS Security Hub, надають візуальне представлення стану безпеки в режимі реального часу, проте деталізація їхніх звітів є нижчою, що обмежує можливості для глибокого аналізу.

Вартість реалізації проведення аудиту безпеки в хмарних середовищах залежить від обраного методу: ручного, автоматизованого або вбудованого. Кожен підхід має свої особливості, які впливають на витрати, як прямі (витрати на інструменти та ресурси), так і непрямі (витрати на час співробітників, використання інфраструктури тощо). Ручне проведення аудиту є безкоштовним з точки зору використання інструментів, але має значні непрямі витрати, пов’язані з оплатою праці спеціалістів. Для розрахунку непрямих витрат враховується середня заробітна плата спеціаліста з інформаційної безпеки в Україні на березень 2025 року, яка становить 40000 грн на місяць при 8-годинному робочому дні та 20 робочих днях [17]. Це дає погодинну ставку 250 грн.

Для виконання 100 перевірок безпеки вручну потрібно витратити 5 хвилин на кожну перевірку та 3 години на створення звіту. Таким чином, витрати на виконання перевірок становлять 2083,33 грн, а створення звіту коштує 750 грн. Загальні витрати складають 2833,33 грн. Ручне проведення аудиту підходить для невеликих середовищ або ситуацій, коли потрібно провести глибокий аналіз складних аспектів безпеки, але цей метод є трудомістким і вимагає високої кваліфікації персоналу, що збільшує час і витрати в міру зростання масштабу перевірок.

Автоматизовані засоби проведення аудиту дозволяють запускати скрипти для перевірки конфігурацій безпеки на локальних чи хмарних ресурсах. Цей підхід зазвичай є безкоштовним, якщо використовуються власні ресурси, однак має непрямі витрати при використанні хмарних обчислювальних потужностей. Наприклад, для запуску перевірок на Amazon EC2 вартість базового екземпляру t2.medium становить 0,0464 USD/година. Нехай вартість реалізації, а саме налаштування ресурсу, конфігурація та встановлення, займе 2 години при песимістичному підході. В такому разі витрати на проведення аудиту в хмарі складуть ≈ 3,88 грн (за курсом на березень 2025 року 1 USD ≈ 41,79 гривні).

Вбудовані інструменти, такі як AWS Security Hub, автоматизують більшість перевірок і інтегруються безпосередньо з хмарною платформою. Прямі витрати включають оплату за кількість перевірок, обробку подій та використання додаткових функцій. Варто зазначити, що Security Hub перевіряє кожен контроль для кожного ресурсу в кожному регіоні. Для розрахунку вартості можна взяти середньостатистичний AWS-акаунт, який розгорнутий у двох регіонах і включає 20 S3 бакетів, 10 EC2 інстансів, 5 IAM ролей, 3 VPC, кожна з яких має 2 Security Groups із 10 правилами в кожній, 2 Network ACLs із 20 правилами в кожній, 3 RDS бази даних, кожна з яких має 2 підключення, та 2 KMS ключі. Загальна кількість перевірок для акаунту з такою інфраструктурою складає ≈ 2480 перевірок. Вартість перевірок розраховується на основі ставки 0.001 USD за кожну перевірку для перших 100,000 перевірок. Таким чином, для 2480 перевірок загальна вартість складе 2480 · 0,001 USD, що приблизно дорівнює 103.64 грн.

Ручне проведення аудиту є найбільш витратним через значні непрямі витрати на оплату праці спеціалістів. Вбудовані інструменти, як AWS Security Hub, мають незначні прямі витрати і не вимагають непрямих витрат. Автоматизоване проведення аудиту має незначні непрямі витрати, якщо використовуються хмарні обчислення, але його вартість значно нижча, ніж у випадку ручного аудиту, що робить цей метод найбільш економним. Це порівняння підсумовано в табл. 2.

Таблиця 2 – Порівняння витрат для різних методів проведення аудиту безпеки хмарних середовищ

Метод проведення аудиту	Прямі витрати, грн	Непрямі витрати, грн
Ручний	0	2833,33
Автоматизований	0	3,88
Вбудований	103,64	0

Висновки

У результаті дослідження було проведено аналіз різних методів проведення аудиту безпеки хмарних середовищ, включаючи ручне, автоматизоване та вбудовані засоби перевірки. Визначено ключові переваги та недоліки кожного з підходів, а також їхню ефективність у різних сценаріях використання. Автоматизовані методи виявилися найбільш ефективними з точки зору швидкості та економічної доцільності, тоді як ручне проведення аудиту забезпечує вищу гнучкість та деталізованість аналізу. Вбудовані засоби моніторингу, які пропонують хмарні провайдери, виявилися корисними для постійного моніторингу змін у конфігураціях, але мають певні обмеження щодо гнучкості та підтримки нестандартних перевірок.

Дослідження показало, що використання автоматизованих інструментів дозволяє значно скоротити час проведення аудиту, знизити витрати та мінімізувати ризики людського фактора. Витрати на автоматизоване проведення аудиту становлять менш ніж 1% від вартості ручного підходу, що робить його значно більш економічно ефективним. Завдяки використанню автоматизованих рішень можна досягти значної економії ресурсів, підвищити точність оцінки безпеки та зменшити ймовірність пропуску критичних вразливостей. При цьому ручне проведення аудиту залишається актуальним у випадках, коли необхідний

індивідуальний підхід до аналізу складних конфігурацій та нестандартних налаштувань безпеки.

Результати дослідження також вказують на необхідність удосконалення підходів до аудиту безпеки шляхом інтеграції методів машинного навчання та штучного інтелекту. Використання алгоритмів аналізу даних дозволить підвищити ефективність автоматизованого аудиту, зокрема через можливість визначення критичності знайдених вразливостей та фільтрації неактуальних перевірок для конкретної організації. Застосування машинного навчання допоможе створити систему адаптивного аудиту, яка зможе ідентифікувати найбільш важливі контролі безпеки, усувати нерелевантні перевірки та знижувати кількість хибнопозитивних результатів. Це дозволить оптимізувати процес аудиту, зменшуючи навантаження на ресурси та підвищуючи його ефективність.

Подальші дослідження можуть бути зосереджені на розробці інтелектуальних систем аналізу ризиків, що здатні самостійно визначати пріоритетність виявлених загроз та рекомендувати заходи з їх усунення. Використання технологій глибокого навчання дозволить створити моделі прогнозування потенційних атак та вразливостей, що забезпечить проактивний підхід до забезпечення безпеки хмарних середовищ. Такі підходи сприятимуть підвищенню рівня захисту даних та критичних ресурсів у хмарній інфраструктурі, забезпечуючи їх відповідність сучасним стандартам безпеки.

Таким чином, результати проведеного дослідження підтверджують необхідність подальшого розвитку автоматизованих та інтелектуальних систем аудиту безпеки хмарних середовищ. Це дозволить не лише підвищити ефективність процесу оцінювання ризиків, а й зробити хмарні сервіси більш безпечними та адаптованими до сучасних викликів кібербезпеки.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. HIPA Journal. IBM: Average Cost of a Healthcare Data Breach Increases to Almost $11 Million. Retrieved from : https://www.hipaajournal.com/2023-cost-healthcare-data-breach/
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Retrieved from : https://www.iso.org/standard/27001
3. GDPR (General Data Protection Regulation). General Data Protection Regulation. Retrieved from :https://gdpr-info.eu/
4. CIS Security. Center for Internet Security. Retrieved from : https://www.cisecurity.org/controls/v8
5. CIS Microsoft 365 Foundations Benchmark v3.1.0. Center for Internet Security, Benchmarks. Retrieved from :https://www.cisecurity.org/cis-benchmarks
6. Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity and Infrastructure Security Agency. Retrieved from : https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency
7. CISA – Official Website. Cybersecurity and Infrastructure Security Agency: Official Site. Retrieved from : https://www.cisa.gov/about

8. CISA Secure Cloud Business Applications. SCuBA project by CISA. Retrieved from : https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
9. Prowler. AWS Security Tool. Retrieved from : https://prowler.com/
10. GitHub: Prowler. Prowler repository on GitHub. Retrieved from : https://github.com/prowler-cloud/prowler
11. GitHub: ScubaGoggles. ScubaGoggles repository. Retrieved from : https://github.com/cisagov/ScubaGoggles
12. AWS Security Hub User Guide. AWS Security Hub: User Guide. Retrieved from : https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html
13. AWS Security Hub. AWS Security Hub. Retrieved from : https://aws.amazon.com/ru/security-hub/
14. Microsoft Secure Score. Microsoft Secure Score. Retrieved from : https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score
15. Microsoft Compliance Manager. Microsoft Compliance Manager. Retrieved from : https://learn.microsoft.com/en-us/purview/compliance-manager
16. GitHub: ScubaGear. ScubaGear repository. Retrieved from : https://github.com/cisagov/ScubaGear
17. Work.ua. Information security specialist: average salary in Ukraine. Retrieved from : https://www.work.ua/en/salary-information+security+specialist/

References

1. HIPA Journal. IBM: Average Cost of a Healthcare Data Breach Increases to Almost $11 Million. Retrieved from : https://www.hipaajournal.com/2023-cost-healthcare-data-breach/
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. Retrieved from : https://www.iso.org/standard/27001
3. GDPR (General Data Protection Regulation). General Data Protection Regulation. Retrieved from :https://gdpr-info.eu/
4. CIS Security. Center for Internet Security. Retrieved from : https://www.cisecurity.org/controls/v8
5. CIS Microsoft 365 Foundations Benchmark v3.1.0. Center for Internet Security, Benchmarks. Retrieved from :https://www.cisecurity.org/cis-benchmarks
6. Cybersecurity and Infrastructure Security Agency (CISA). Cybersecurity and Infrastructure Security Agency. Retrieved from : https://en.wikipedia.org/wiki/Cybersecurity_and_Infrastructure_Security_Agency
7. CISA – Official Website. Cybersecurity and Infrastructure Security Agency: Official Site. Retrieved from : https://www.cisa.gov/about
8. CISA Secure Cloud Business Applications. SCuBA project by CISA. Retrieved from : https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
9. Prowler. AWS Security Tool. Retrieved from : https://prowler.com/
10. GitHub: Prowler. Prowler repository on GitHub. Retrieved from : https://github.com/prowler-cloud/prowler
11. GitHub: ScubaGoggles. ScubaGoggles repository. Retrieved from : https://github.com/cisagov/ScubaGoggles
12. AWS Security Hub User Guide. AWS Security Hub: User Guide. Retrieved from : https://docs.aws.amazon.com/securityhub/latest/userguide/what-is-securityhub.html

13. AWS Security Hub. AWS Security Hub. Retrieved from : https://aws.amazon.com/ru/security-hub/
14. Microsoft Secure Score. Microsoft Secure Score. Retrieved from : https://learn.microsoft.com/en-us/defender-xdr/microsoft-secure-score
15. Microsoft Compliance Manager. Microsoft Compliance Manager. Retrieved from : https://learn.microsoft.com/en-us/purview/compliance-manager
16. GitHub: ScubaGear. ScubaGear repository. Retrieved from : https://github.com/cisagov/ScubaGear
17. Work.ua. Information security specialist: average salary in Ukraine. Retrieved from : https://www.work.ua/en/salary-information+security+specialist/