УДК 004.8:004.056
DOI: 10.31673/2409-7292.2025.012256

Скоринович Б.В., Лах Ю.В.

АНАЛІЗ МЕТОДІВ МОНІТОРИНГУ СТАНУ БЕЗПЕКИ В ХМАРНОМУ СЕРЕДОВИЩІ

Стрімке поширення хмарних обчислень зумовлює появу нових викликів у сфері інформаційної безпеки. Організації стикаються з необхідністю забезпечення надійного захисту даних і додатків у динамічних, мультихмарних середовищах. У статті розглянуто актуальні питання забезпечення безпеки даних у хмарних середовищах із урахуванням зростаючої кількості некоректних конфігурацій, які становлять основну частку інцидентів безпеки. Розглянуто три ключові підходи: управління станом безпеки хмарних середовищ (CSPM), захист хмарних робочих навантажень (CWPP) та платформи захисту хмарних додатків (CNAPP). Детально описано функціональні можливості, переваги та обмеження кожного підходу, наведено приклади їх практичного застосування. Окрему увагу приділено ролі штучного інтелекту та машинного навчання у процесі моніторингу. Продемонстровано, як ШІ/МН допомагають виявляти приховані загрози й аномалії, прискорювати обробку великих обсягів журналів, а також впроваджувати автоматизоване реагування. Наведено приклади хмарних сервісів (Amazon GuardDuty, Azure Defender, Google Security Command Center), що вже реалізують розвинені ML-модулі для виявлення складних багатоступеневих атак і нетипових патернів у поведінці користувачів. Проаналізовано ключові виклики впровадження цих рішень — від надмірної кількості сповіщень у CSPM, складності розгортання агентів у CWPP і ризиків залежності від одного постачальника в CNAPP. Водночас наголошується, що правильно налаштована система моніторингу у поєднанні з людською експертизою може істотно зміцнити хмарну безпеку та мінімізувати ризики інцидентів. У статті підкреслюється необхідність комплексного підходу, що охоплює різні рівні захисту та демонструється, як залучення ШІ/МН сприяє формуванню проактивних, динамічних стратегій безпеки у хмарних середовищах

Ключові слова: безпека хмарних обчислень, штучний інтелект (ШІ/AI), машинне навчання (МН/ML), CSPM, CWPP, CNAPP, кібербезпека.

Вступ

Хмарні обчислення стали невід'ємною складовою сучасної IT-інфраструктури, ґрунтовно трансформувавши підходи до зберігання, управління й забезпечення безпеки даних. Водночас така інтеграція зумовила появу нових складних викликів у сфері інформаційної безпеки. Організації нерідко зіштовхуються з труднощами у підтримці належного рівня захищеності в динамічних, мультихмарних середовищах (наприклад, AWS, Azure, GCP). Некоректна конфігурація хмарних сервісів залишається однією з провідних причин безпекових інцидентів: результати опитувань свідчать, що операційні команди "надзвичайно стурбовані" помилками у налаштуванні й феноменом так званого «конфігураційного дрейфу», які призводять до появи додаткових вразливостей у системі безпеки [1]. Згідно з оцінками Gartner, саме некоректна конфігурація хмарних сервісів та помилки користувачів становлять переважну більшість випадків порушень безпеки хмарних середовищ (близько 80%) і призведуть до 99% відмов у хмарних середовищах до 2025 року [2]. Така велика кількість факторів ризику призводить до критичної проблеми: як організації можуть безперервно спостерігати за станом безпеки своїх хмарних середовищ та керувати ним, щоб запобігти витокам даних та іншим інцидентам безпеки? Постає нагальна потреба у впровадженні автоматизованих, інтелектуальних методах безперервного моніторингу стану безпеки хмарних середовищ, виявлення вразливостей або аномалій у режимі реального часу та усунення проблем до того, як вони призведуть до компрометації системи.

Аналіз літературних джерел та формулювання проблеми

Усвідомлюючи ці виклики, науковці та провідні компанії галузі приділяють значну увагу моніторингу стану безпеки хмарних середовищ. Галузеві опитування (наприклад, звіт Cloud Security Alliance за 2021 рік) підкреслюють, що некоректні конфігурації та недостатня прозорість є головними загрозами безпеці в хмарних середовищах [1]. Академічні дослідження також наголошують на цій тенденції. Зокрема, Guffey and Li (2023) описують, як некоректні конфігурації хмарних сервісів призвели до численних випадків витоку даних з корпоративних систем, і обговорюють рішення для зменшення цих загроз [3]. Такі висновки

відображають широкий консенсус: безперервний моніторинг на предмет некоректної конфігурації та відповідності нормативним вимогам має першорядне значення в хмарних середовищах.

Щоб протидіяти цим загрозам індустрія хмарної безпеки розробила інструменти класу управління станом безпеки у хмарі (CSPM, Cloud Security Posture Management) для автоматичної перевірки відповідності конфігурацій хмарної інфраструктури найкращим галузевим практикам та вчасному сигналізуванню про потенційно вразливі місця. У наукових публікаціях триває активне обговорення ефективності CSPM. Зокрема, Jimmi (2023) пропонує детальний огляд методик CSPM, підкреслюючи, що сучасні рішення передбачають не лише використання вбудованих хмарних сервісів, а й «автоматизацію на основі штучного інтелекту» для виявлення загроз [4]. Зі свого боку, провідні хмарні провайдери (наприклад, AWS, Microsoft Azure, Google Cloud) впровадили власні сервіси для управління станом безпеки (зокрема, AWS Config та Security Hub, Azure Policy і Microsoft Defender for Cloud, Google Cloud Security Command Center), а їхня технічна документація містить суттєві рекомендації щодо належних практик конфігурування.

Ще один напрям сучасних досліджень зосереджений на так званих платформах захисту хмарних робочих навантажень (Cloud Workload Protection Platforms, CWPP), які виходять за межі простого контролю налаштувань і забезпечують захист хмарних обчислювальних ресурсів (віртуальних машин, контейнерів, безсерверних функцій, тощо) безпосередньо під час виконання цих процесів. Через те, що організації використовують різноманітні робочі навантаження, наукові праці дедалі частіше фокусуються на здатності рішень CWPP виявляти та блокувати активні загрози у хмарних системах. Наприклад, у дослідженні Coppola та ін. (2023) описано прототип поєднаної системи CSPM/CWPP, що інтегрує сигнали загроз (threat intelligence feeds) і використовує NIST Cybersecurity Framework для класифікації заходів контролю безпеки. Розроблений ними дизайн використовує сервіси хмарних провайдерів (наприклад, AWS GuardDuty для сповіщень про загрози) для розширення можливостей моніторингу [5].

Тим часом, галузевий аналіз, проведений Gartner та іншими, показав, що CWPP еволюціонує до більш уніфікованих рішень; у 2021 році Gartner ввів термін CNAPP (Cloud-Native Application Protection Platform), щоб позначити платформи, які об'єднують CSPM, CWPP та інші функціональні модулі [6]. Останні публікації та технічні документи галузевих компаній-гігантів (наприклад, від Gartner, IDC та Cloud Security Alliance) розглядають CNAPP як цілісний підхід, і постачальники швидко адаптували цю концепцію у своїх продуктових пропозиціях. Microsoft Defender for Cloud, Palo Alto Prisma Cloud, Orca Security, Wiz та інші часто згадуються як приклади в галузевих статтях про те, як CNAPP об'єднує раніше розрізнені інструменти.

Роль штучного інтелекту (ШІ) та машинного навчання (МН) у моніторингу безпеки хмарних середовищ нині привертає дедалі більшу увагу наукової спільноти. Оглядові праці, зокрема Choubey, R. (2023), систематизують широкий спектр застосувань МН для захисту хмари — від виявлення вторгнень і аномалій до прогнозування вразливостей і оцінювання стану безпеки [7]. Результати цих досліджень свідчать, що застосування ШІ/МН дає змогу суттєво підвищити точність виявлення загроз у хмарних середовищах та зменшити кількість хибних спрацювань, що також узгоджується з висновками експертів з кібербезпеки. У блозі компанії Microsoft (2024), присвяченому безпеці хмарних технологій, відзначається, що все більше організацій впроваджують ШІ/МН для посиленого захисту хмарних середовищ з метою ефективнішого виявлення, аналізу й реагування на загрози [8]. Аналогічно, в технічній документації AWS наголошується на важливості МН у сервісі GuardDuty, який використовує алгоритми машинного навчання для безперервного аналізу типової поведінки користувачів у хмарі та виявлення аномалій, що можуть свідчити про кібератаку [9].

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

Підсумовуючи, останні наукові публікації й аналітичні звіти свідчать про те, що безперервний автоматизований моніторинг і управління станом безпеки з використанням інтелектуальної аналітики стає ключовим напрямом розвитку хмарної безпеки.

Мета роботи та цілі дослідження

Основною метою цього дослідження є проведення поглибленого аналізу методів моніторингу стану безпеки в хмарних середовищах різних постачальників послуг. Це передбачає вивчення сучасних практик (CSPM, CWPP, CNAPP) та оцінку того, як новітні технології, такі як ШІ та МН, покращують моніторинг безпеки хмарних середовищ.

Для досягнення зазначеної мети передбачається виконати такі ключові завдання:

- Дослідити сучасні методи CSPM, CWPP і CNAPP (архітектура, функції, вирішувані проблеми безпеки), виявити їхні переваги та обмеження на прикладі реальних хмарних платформ (AWS, Azure, GCP).
- Дослідити застосування штучного інтелекту (ШІ) і машинного навчання (МН) для моніторингу стану безпеки хмарних середовищ, зокрема, як ці технології покращують виявлення загроз, розпізнавання аномалій та автоматизацію реагування.
- Синтезувати отримані результати, сформулювати висновки щодо ефективних стратегій моніторингу стану безпеки та надати рекомендації для організацій, що впроваджують рішення CSPM/CWPP/CNAPP та використовують ШІ для моніторингу.

Результати досліджень

***Cloud Security Posture Management (CSPM*).** Управління станом безпеки в хмарних середовищах (Cloud Security Posture Management, CSPM) охоплює технології, що забезпечують безперервне виявлення, оцінювання та усунення неправильних налаштувань у хмарній інфраструктурі [10]. Як правило, CSPM-рішення інтегруються з API хмарних провайдерів, щоб автоматично отримувати відомості про конфігурації та ресурси у всьому середовищі. Надалі ці налаштування звіряються з рекомендованими практиками безпеки, вимогами нормативної відповідності та відомими сценаріями загроз. Зазвичай CSPM пропонується у форматі програмної платформи чи сервісу, який може охоплювати кілька облікових записів або хмарних служб для формування уніфікованого огляду ризиків. Наприклад, CSPM-інструмент через API хмарного провайдера отримує параметри конфігурації (встановлення доступу до сховища, політики IAM, правила мережевих брандмауерів тощо) та перевіряє їх на наявність вразливостей або невідповідностей політикам (зокрема, загальнодоступні сховища S3 або надмірно ліберальні мережеві правила). Сучасні CSPM-рішення, зазвичай, працюють у безперервному або майже реальному часі, на відміну від періодичних ручних перевірок. Така модель роботи дає змогу ефективно відстежувати зміни у хмарній інфраструктурі й оперативно реагувати на потенційні ризики.

Переваги CSPM:

● Комплексна видимість: CSPM надають повну видимість хмарних активів і конфігурацій, автоматично виявляючи ресурси та зв'язки між ними. Це критично важливо для ідентифікації ризикованих налаштувань (відкриті порти, вимкнене журналювання, незашифровані дані) у складних мультихмарних середовищах.

● Виявлення конфігураційних помилок і контроль відповідності: CSPM постійно перевіряє конфігурації на відповідність галузевим стандартам (наприклад, CIS) і нормативним вимогам (PCI DSS, HIPAA, GDPR), сповіщаючи про порушення. Це дозволяє проактивно усувати проблеми (необмежений доступ, некоректні дозволи) до їх використання зловмисниками, а також спрощує звітування про стан безпеки.

● Пріоритезація ризиків: Розширені CSPM-рішення пріоритезують виявлені проблеми, оцінюючи вразливість, чутливість даних і потенційний радіус ураження. Це дозволяє командам фокусуватися на усуненні найбільш критичних загроз.

● Автоматизація усунення: Багато CSPM-платформ пропонують автоматизоване усунення проблем: від покрокових інструкцій до автоматичного виправлення конфігурацій (за

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

наявності дозволів). Це скорочує час вразливості. Деякі інтегруються з DevOps-конвеєрами, запобігаючи потраплянню небезпечних конфігурацій у production.

● Мультихмарність: CSPM ідеально підходить для мультихмарних і гібридних середовищ, агрегуючи дані про стан безпеки з різних платформ (AWS, Azure, Google Cloud, локальні системи) через API, уніфікуючи представлення ризиків.

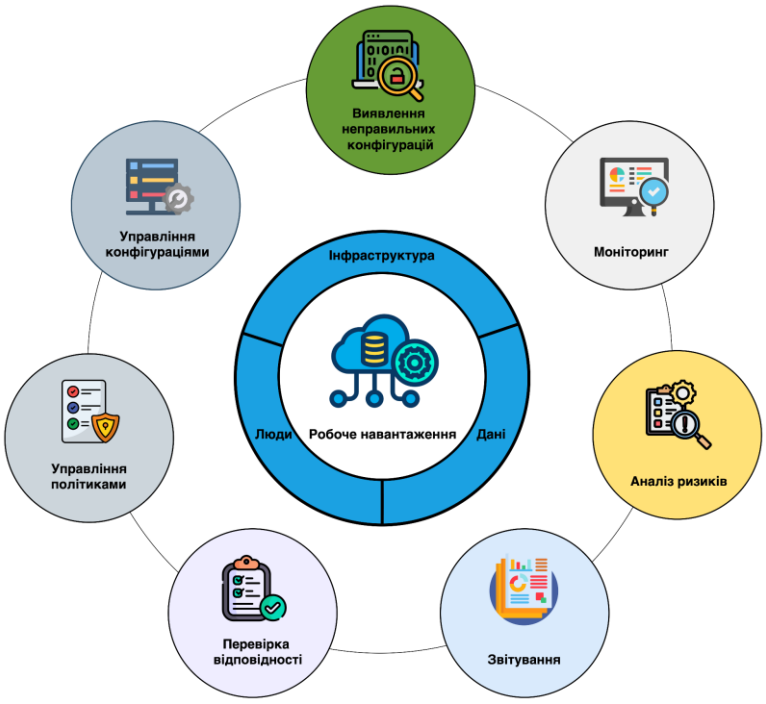

Рис 1. Ключові можливості CSPM
(основний фокус зміщений на інфраструктуру, людей та дані).

Обмеження CSPM:

● Зосередженість на конфігурації: CSPM зосереджений на конфігураціях і політиках, ефективно виявляючи невідповідності, але не здійснює глибокий моніторинг поведінки в реальному часі. Це означає, що CSPM може не виявити активні загрози, які не пов'язані з явними помилками конфігурації (для цього потрібні CWPP).

● Надмірна кількість сповіщень: CSPM-інструменти можуть генерувати велику кількість сповіщень, особливо у великих середовищах, що ускладнює визначення пріоритетів. Хоча новіші рішення покращують контекст і пріоритезацію, ризик "шуму" залишається без ретельного налаштування.

● Складнощі з усуненням недоліків: Автоматичне виправлення конфігурацій може бути ризикованим, потенційно порушуючи роботу залежних сервісів. Тому часто CSPM використовують у режимі моніторингу з ручним підтвердженням виправлень, що уповільнює реагування.

● Потреба в експертизі та інтеграції: Розгортання CSPM вимагає інтеграції з усіма хмарними обліковими записами та сервісами, а також експертних знань для налаштування політик, порогових значень та оновлень, щоб уникнути хибних спрацювань і прогалин у моніторингу.

CSPM є фундаментальним інструментом для забезпечення безпеки хмарних середовищ, що безперервно перевіряє хмарні ресурси на предмет некоректних конфігурацій. Вбудовані засоби (AWS Security Hub, Azure Defender, Google Security Command Center) та сторонні рішення (Prisma Cloud, Wiz, Orca) виявляють відкриті порти, надмірні права доступу, відсутність шифрування або застаріле програмне забезпечення. Виявлені проблеми

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

оформлюються як сповіщення або тікети, які усуває відповідальна DevOps-команда або команда безпеки. Згодом організації відстежують динаміку кількості критичних вразливостей і демонструють прогрес у безпеці за допомогою звітів CSPM. Таким чином, CSPM забезпечує превентивний захист і своєчасне виявлення помилок конфігурації, тримаючи інфраструктуру в межах належних практик.

Cloud Workload Protection Platform (CWPP). Платформа захисту хмарних робочих навантажень – це рішення, розроблене для забезпечення безпеки робочих навантажень у хмарному середовищі, зокрема віртуальних машин, контейнерів і безсерверних функцій, шляхом виявлення та блокування загроз на рівні самого навантаження [10]. Якщо CSPM зосереджується переважно на налаштуваннях хмарного середовища, то CWPP фокусується на захисті під час виконання (runtime security), охоплюючи як хмарні, так і локальні ресурси. CWPP-рішення використовують агенти, що встановлюються на робочі навантаження, та/або безагентні методи (сканування знімків, аналіз хмарних журналів) для моніторингу активності, виявлення шкідливого ПЗ та забезпечення політик безпеки. Сучасні CWPP часто поєднують обидва підходи. Результати моніторингу та аналітика загроз доступні через центральну консоль управління.

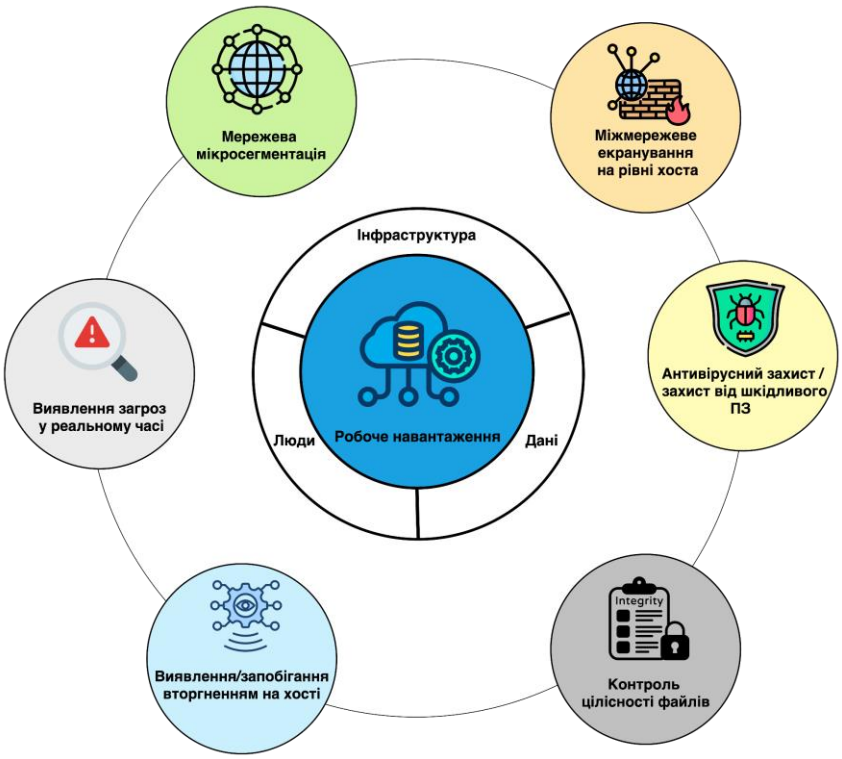

Рис 2. Ключові можливості CWPP
(основний фокус зміщений на робоче навантаження та процеси всередині).

CWPP забезпечує управління вразливостями (сканування на наявність вразливостей і відсутніх патчів), посилення конфігурації (безпечні налаштування ОС та ін.) та виявлення/реагування на загрози в режимі реального часу. CWPP постійно моніторить робочі навантаження, виявляючи аномальну поведінку (наприклад, нетипові процеси на ВМ) та реагуючи на неї (зупинка процесу, сповіщення). У контейнерних середовищах CWPP інтегрується з оркестраторами (наприклад, Kubernetes) для виявлення специфічних загроз (виходи з контейнера, підозрілий трафік).

Переваги CWPP:

- Виявлення загроз у режимі реального часу: CWPP виявляє активні загрози на рівні робочого навантаження (наприклад, шкідливий код або нетипову поведінку процесів), що не

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

помітні за статичного аналізу конфігурацій. Зокрема, воно може виловлювати спроби майнінгу криптовалют чи зловмисні API-запити в хмарі.

● Універсальний захист: CWPP забезпечує уніфікований підхід до безпеки для віртуальних машин, контейнерів та безсерверних функцій, незалежно від обраного хмарного провайдера. Це особливо цінне у мультихмарних сценаріях з різноманітними типами сервісів.

● Автоматизоване реагування: Чимало CWPP-рішень можуть ізолювати скомпрометований вузол, завершувати зловмисні процеси або блокувати небезпечні виконавчі файли. Завдяки інтеграції із системами SIEM/SOAR, вони також запускають сценарії розширеного реагування (playbooks), мінімізуючи час між виявленням і нейтралізацією загрози.

● Розвинені засоби безпеки: До арсеналу CWPP зазвичай входять IDS/IPS, антивірусні механізми, списки дозволеного ПЗ (allow-listing) і моніторинг цілісності. Таке “нашарування” захисту на рівні обчислювальних ресурсів суттєво підсилює виявлення критичних загроз (на кшталт спроб підвищення привілеїв або розгортання з вразливим контейнерним образом).

● Контекстні сповіщення: Завдяки моніторингу реальних подій, CWPP генерує високоточні сповіщення з меншою кількістю хибних спрацьовувань, а також може корелювати події для виявлення складних атак.

● Глибока видимість завдяки агентам (за потреби): Агенти забезпечують глибокий моніторинг процесів, мережевих з'єднань та системних викликів, що недоступно для мережевих засобів захисту, особливо при шифруванні трафіку.

Обмеження CWPP:

● Накладні витрати: Агентські CWPP вимагають ресурсів (ЦП, пам'ять) і зусиль на розгортання/управління, що може бути проблематично в динамічних середовищах.

● Прогалини безагентного підходу: Безагентні методи (наприклад, періодичне сканування) не завжди здатні виявляти загрози в реальному часі чи атаки в оперативній пам’яті. Окрім того, робочі навантаження безсерверної архітектури (serverless) швидко виникають і зникають, що ускладнює їхнє постійне відстеження..

● Складність управління. Інтеграція CWPP у мультихмарних середовищах вимагає складних налаштувань і ретельного моніторингу. Некоректні політики у самому CWPP можуть спричинити або надмірну кількість сповіщень, або пропуск інцидентів, якщо налаштування виявляться занадто ліберальними.

● Брак контексту: CWPP детально показує події у конкретних робочих навантаженнях, але не завжди дає розуміння загальної хмарної конфігурації. Це може ускладнити пошук причин вразливостей, пов’язаних із неправильними налаштуваннями, що перебувають поза межами окремого навантаження.

● Реактивний підхід: Історично, деякі CWPP були більш реактивними (реагували на загрози після їх виникнення), а не проактивними. Сучасні підходи зміщують акцент на превентивність (сканування в CI/CD), але це не завжди реалізовано.

● Вартість: Комерційні CWPP-рішення можуть бути затратними (оплата за кожну віртуальну машину чи контейнер). При дуже великих масштабах це може обмежувати повноцінне розгортання агентів, що залишає деякі вузли вразливими.

Компанії використовують CWPP для моніторингу й захисту своїх хмарних робочих навантажень під час виконання (runtime). Наприклад, в AWS можуть одночасно працювати віртуальні машини (EC2), Kubernetes-кластери (EKS) і серверлес-функції (Lambda). CWPP-рішення (як-от Trend Micro Cloud One або штатні засоби AWS) встановлюють агенти на EC2 та інтегруються з Kubernetes, щоби виявляти зловмисний код чи нетипову поведінку процесів (скажімо, завантаження підозрілої бінарної програми). У разі виявлення шкідливого ПЗ CWPP негайно надсилає сповіщення або блокує інфікований вузол від мережі. CWPP також застосовується в Kubernetes для контролю поведінки контейнерів.

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

Реальний приклад: злам хмарної інфраструктури Capital One у 2019 році стався через те, що зловмисник використав некоректно налаштований WAF для доступу до метаданих AWS та викрадення даних з кошика S3. CSPM міг би виявити некоректну конфігурацію (що було однією з проблем), але CWPP міг би виявити незвичну поведінку на робочому навантаженні (контейнер WAF, що робить нетипові запити). На практиці компанії тепер використовують обидва рішення – CSPM для виявлення некоректних конфігурацій (запобігання проникненню) та CWPP для виявлення будь-якої шкідливої активності (виявлення бічного переміщення або ексфільтрації даних). Ця взаємодоповнюваність є причиною того, що індустрія почала переходити до уніфікованих платформ (CNAPP).

Cloud-Native Application Protection Platform (CNAPP). Хмарна платформа для захисту додатків - це інтегрований підхід, що об'єднує CSPM, CWPP та інші інструменти хмарної безпеки в єдину платформу[11]. CNAPP забезпечує консолідований захист хмарних додатків, включаючи моніторинг конфігурацій, захист робочих навантажень під час виконання, управління правами доступу (Cloud Infrastructure Entitlement Management, CIEM) та, часто, функції DevSecOps. Платформа інтегрується з хмарними API та використовує агенти/сенсори для моніторингу, а ключовою особливістю є обмін даними між компонентами для кореляції подій і забезпечення єдиного уявлення про ризики. Ключові можливості та архітектурні аспекти платформ CNAPP в деталях наведені в таблиці 1.

Таблиця 1

Ключові можливості та архітектурні аспекти платформ CNAPP

Можливість/Аспект	**Опис**
Уніфікована панель та модель даних	Інтеграція даних зі сканувань конфігурації, телеметрії робочих навантажень, сканувань вразливостей, аналізу ідентифікаційних даних в єдине сховище. Забезпечує єдиний інтерфейс для видимості загроз у різних хмарних середовищах і навантаженнях, усуваючи розрізненість між безпекою конфігурацій і робочих навантажень. Сприяє співпраці DevSecOps.
Інтеграція з DevSecOps ("Shift-Left")	Вбудовування безпеки на ранніх етапах розробки. Сканування коду, образів контейнерів, IaC-конфігурацій під час розробки та в CI/CD-конвеєрах (SAST/DAST). Виявлення та виправлення вразливостей до розгортання.
Мультихмарна та гібридна підтримка	Підтримка різних публічних хмар (Azure, AWS, Google Cloud) і локальних середовищ в єдиному рішенні. Забезпечує централізоване управління безпекою незалежно від розташування навантажень.
Інтегрований CIEM	Аналіз ролей, дозволів і використання для виявлення ризикованих призначень привілеїв (Cloud Infrastructure Entitlement Management). Забезпечення принципу найменших привілеїв, виявлення аномалій у використанні ідентифікаторів.
Контекстне виявлення	Кореляція даних з різних рівнів (конфігурації, робочі навантаження) для надання контекстних сповіщень. Автоматичне об'єднання пов'язаних подій в інциденти, зменшення шуму, пріоритезація загроз.
Спрощені операції	Консолідація інструментів безпеки в єдину платформу. Зменшення складності, витрат, дублювання даних, спрощення розгортання агентів. Автоматичне масштабування та оновлення (для хмарних CNAPP).

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

Переваги CNAPP:

● Цілісна безпека: CNAPP охоплює повний життєвий цикл хмарних рішень: від розробки (shift-left) і перевірки конфігурацій (CSPM) до захисту під час виконання (CWPP). Завдяки цьому зменшується ймовірність, що прогалини у безпеці залишаться непоміченими, оскільки різні модулі інформують один одного (наприклад, уразливості впливають на рейтинг ризику, а налаштування хмари уточнюють пріоритети захисту).

● Покращене виявлення та менше шуму: Кореляція даних з різних джерел (CSPM, CWPP) зменшує хибні спрацювання та покращує виявлення реальних атак, надаючи контекстні сповіщення.

● Підтримка DevSecOps: Інтеграція CNAPP у процеси розробки (CI/CD) дозволяє виявляти недоліки безпеки на ранніх етапах. Розробники отримують зворотний зв'язок у власних середовищах, а команди безпеки контролюють процес розгортання. У результаті покращується якість базової безпеки та зменшується кількість інцидентів у продуктивному середовищі.

● Єдина платформа для мультихмарних рішень.: Єдиний набір політик і централізована оцінка стану безпеки для різних хмарних провайдерів (AWS, Azure, GCP тощо) спрощують управління та звітність.

● Зниження складності та вартості: Консолідація інструментів в єдину платформу (потенційно) зменшує витрати, спрощує управління та навчання персоналу.

Обмеження CNAPP:

● Недостатня зрілість та інтеграція: Оскільки CNAPP досить нова концепція, багато рішень складаються з окремих модулів, які можуть бути ще не повністю узгоджені в єдину платформу. Реально це може виглядати як "кілька продуктів в одному", а не справді злитий продукт.

● Складність впровадження: Впровадження CNAPP – складний проєкт, що вимагає координації різних команд (адміністратори, DevOps, розробники) та значного часу.

● Залежність від одного вендора. Використання єдиної платформи створює залежність; збій або слабкість одного з компонентів може мати широкі наслідки.

● Великі обсяги даних: CNAPP охоплює чимало джерел: логи, конфігурації, сканування вразливостей, дані ідентифікації тощо. Управління такою кількістю інформації потребує серйозних ресурсів і може призвести до значних витрат на зберігання, передачу та обробку.

● Хибне відчуття безпеки: Хоча CNAPP покриває багато аспектів хмарної безпеки, він не є панацеєю. Компаніям все одно потрібні кваліфіковані фахівці для тлумачення результатів, реагування на інциденти та правильного налаштування інструменту. Нові методи атак можуть обходити автоматизовані засоби, тож людський досвід залишається критично важливим.

На практиці CNAPP впроваджуються організаціями, які прагнуть зрілості у сфері безпеки хмарних додатків. Типовий приклад: технологічна компанія, яка використовує Kubernetes у мультихмарному середовищі, вирішує замінити свої окремі інструменти безпеки (наприклад, сканер образів Kubernetes, інструмент перевірки конфігурації хмари та антивірусний агент для хмарних робочих навантажень) на єдину платформу CNAPP. Вони розгортають щось на зразок Prisma Cloud або Microsoft Defender for Cloud. На етапі розробки інтеграція CNAPP з CI/CD сканує образи контейнерів на наявність вразливостей, а файли IaC – на наявність некоректних конфігурацій, запобігаючи розгортанню небезпечного коду. Після розгортання коду компонент CSPM платформи CNAPP постійно відстежує конфігурацію хмари (облікові записи AWS, підписки Azure тощо) на предмет будь-якого дрейфу або некоректної конфігурації (можливо, команда розробників запустила новий хмарний сервіс без належних налаштувань – CNAPP позначить це). Одночасно компонент CWPP працює на реальних робочих навантаженнях, відстежуючи аномалії або атаки (якщо хтось використовує вразливість нульового дня в додатку, CWPP може виявити нетиповий процес, який він породжує). Модуль CIEM стежить за ідентифікаторами – наприклад, він може помітити, що

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

обліковий запис служби раптово отримує права адміністратора, і надіслати сповіщення. Усі ці сповіщення та висновки надходять до єдиної центральної консолі.

Таблиця 2

Порівняльна таблиця CSPM, CWPP і CNAPP

Назва методу	Основний фокус	Переваги	Обмеження	Приклади інструментів
CSPM	Конфігурація хмарної інфраструктури та відповідність політикам безпеки.	Всеосяжна видимість хмарних активів і конфігурацій. Автоматичне виявлення некоректних конфігурацій і невідповідностей стандартам. Пріоритезація ризиків. Спрощення забезпечення відповідності нормативним вимогам.	Фокус на статичних конфігураціях, обмежене виявлення загроз у реальному часі. - Можливе перевантаження сповіщеннями ("шум"). - Складнощі автоматизації виправлень. Потреба в експертизі для налаштування.	AWS Security Hub, Azure Security Center (Defender for Cloud), Google Cloud Security Command Center, Prisma Cloud, Orca Security
CWPP	Захист робочих навантажень (ВМ, контейнери, безсерверні функції) під час виконання.	- Виявлення загроз у реальному часі на рівні робочого навантаження. Універсальний захист для різних типів навантажень. - Автоматизоване реагування на інциденти. - Глибокий контроль безпеки (HIDS/HIPS, антивірус, контроль додатків). Контекстні сповіщення.	Накладні витрати на розгортання та управління агентами (для агентських рішень). Прогалини у видимості при безагентних підходах. Складність управління в мультихмарних середовищах. Відсутність контексту хмарної інфраструктури. Реактивний характер (деякі рішення).	Trend Micro Cloud One, CrowdStrike Falcon, Aqua Security, Sysdig Secure, Palo Alto Prisma Cloud, AWS GuardDuty, Wiz, Orca
CNAPP	Інтегрована платформа для забезпечення безпеки хмарних додатків протягом усього життєвого циклу (включаючи CSPM, CWPP та інші функції).	- Цілісний підхід до хмарної безпеки. Покращене виявлення загроз і зменшення "шуму" завдяки кореляції даних. Підтримка DevSecOps. Узгодженість політик у мультихмарних середовищах. Зниження складності та потенційної вартості.	Відносна незрілість ринку, потенційні проблеми інтеграції компонентів. Складність розгортання Залежність від одного постачальника. - Потенційно високі вимоги до ресурсів та обсягів даних. Ризик хибного відчуття безпеки.	Microsoft Defender for Cloud, Prisma Cloud, Wiz, Orca Security, Lacework, Sysdig Secure

Використання ШІ та МН у моніторингу стану безпеки хмарних сервісів

Штучний інтелект (ШІ) та машинне навчання (МН) стали потужними каталізаторами в моніторингу стану безпеки хмарних середовищ. Враховуючи величезний масштаб і складність хмарних середовищ (з незліченною кількістю подій, журналів і конфігурацій, що швидко змінюються), методи ШІ/МН є необхідними для виявлення патернів і аномалій, які люди або прості системи, що базуються на правилах, можуть пропустити. ШІ та МН може значно покращити ключові механізми моніторингу стану безпеки в хмарі, особливо при виявленні загроз, аномалій та автоматизованій відповіді на інциденти.

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

Покращене виявлення загроз. ШІ та МН суттєво розширюють можливості виявлення загроз у хмарних середовищах, адже вони аналізують великі масиви даних, визначаючи, що є “нормальною” поведінкою, і виокремлюючи будь-які відхилення від неї. Постачальники хмарних послуг вбудували МН у свої власні служби безпеки – яскравим прикладом є Amazon GuardDuty, який "використовує штучний інтелект (ШІ), машинне навчання (МН), виявлення аномалій та аналітику загроз, щоб допомогти захистити облікові записи, робочі навантаження та дані AWS" [9]. Навчаючись на мільярдах подій (виклики API, мережеві потоки, спроби входу), моделі GuardDuty можуть ідентифікувати складні, багатоетапні моделі атак (наприклад, повільне бічне переміщення або ланцюжок підвищення привілеїв), які можуть не ініціювати спрацювання жодного окремого правила [9].

Крім того, моделі на основі МН здатні постійно вдосконалюватися: спостерігаючи дедалі більший потік даних (включно з підтвердженими прикладами атак), вони поступово відточують уміння розрізняти шкідливу та легітимну активність. У науково-дослідницькому контексті методи глибинного навчання неодноразово застосовувались для виявлення проникнень у хмарні середовища і показали вагомі результати. Наприклад, в одному з досліджень використання глибинних нейронних мереж для виявлення кібератак у хмарі дозволило виявити, що обмін напрацьованими шаблонами атак між різними системами покращує показники детектування [4]. Основна перевага МН у цьому випадку полягає в здатності поєднувати та аналізувати тонкі сигнали з різних потоків логів чи телеметрії, що є складним завданням для статичних правил виявлення.

При цьому не лише хмарні провайдери впроваджують подібний підхід: сторонні CNAPP-рішення також використовують МН у своїх механізмах моніторингу загроз. Зокрема, Microsoft Defender for Cloud поєднує “просунуту безпекову аналітику ШІ” з розвідданими Microsoft, щоб забезпечити контекстуальне виявлення аномальних дій у хмарних ресурсах. Завдяки цьому можливо ідентифікувати таку активність, як майнінг криптовалют або нетипові патерни доступу до даних, які важко було б виявити методами, побудованими виключно на сигнатурах.

Підсумовуючи, виявлення загроз у хмарі на основі ШІ/МН означає швидше виявлення атак (часто в режимі реального часу) і здатність виявляти нові, нетипові методи зловмисників, орієнтуючись насамперед на поведінкові сигнали, а не виключно на вже відомі шаблони чи сигнатури.

Інтелектуальне розпізнавання аномалій. Хмарні середовища генерують величезний обсяг логів (подій, викликів API, мережевих з’єднань), і саме методи машинного навчання здатні ефективно визначати базову «нормальну» активність і вирізняти відхилення, що можуть свідчити про проблеми з безпекою. Прикладом такої аномалії може бути IAM-користувач, який раптово починає здійснювати API-запити о третій ночі з незнайомої IP-адреси, або різкий стрибок мережевого трафіку до бази даних, яка зазвичай працює у стабільному режимі. Такі патерни можуть не збігатися з відомою сигнатурою загрози, проте все одно викликають підозру.

Методи виявлення аномалій на основі ШІ (наприклад, кластеризація, виявлення викидів, прогнозування часових рядів) можуть вивчати нормальні робочі діапазони для кожного ресурсу та сповіщати, коли щось суттєво відхиляється. Низка рішень CSPM починають інтегрувати такі механізми виявлення аномалій, щоб зменшити кількість помилкових сповіщень і додати більше контексту. Скажімо, модель МН може «запам’ятати», що адміністратор зазвичай створює не більше п’яти віртуальних машин одночасно; якщо ж раптом у системі з’являється 50 VM за короткий проміжок часу, це розцінюється як аномалія (причиною може бути неправильна автоматизація або й шкідливий скрипт).

У науковому середовищі дослідники застосовують методи безнаглядного навчання (unsupervised ML) для виявлення інсайдерських загроз або неправильного використання хмарних ресурсів, створюючи типові профілі поведінки користувачів і виявляючи відхилення від цих профілів [12]. Такий підхід істотно зменшує «шум», оскільки фокусує увагу безпекової

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

команди на дійсно нетипових діях, що кардинально відрізняються від загальної картини. Крім того, застосування ШІ допомагає зменшити кількість помилкових сповіщень: система машинного навчання, аналізуючи контекст, може встановити, що певна незвична подія насправді є безпечною у світлі інших чинників, тоді як механізм на базі жорстких правил виявив би її автоматично.

Аналітика поведінки користувачів і сутностей (User and Entity Behavior Analytics, UEBA) – це концепція, яка часто реалізується за допомогою МН у хмарному моніторингу – вивчення нормальних моделей використання для кожного користувача/сервісу та виявлення аномалій. Постачальники хмарних послуг, такі як Azure, мають функцію виявлення аномалій у таких службах, як Azure AD Identity Protection та Azure Sentinel, а GuardDuty від AWS має функцію виявлення аномалій, наприклад, незвичних моделей викликів API або спроб входу. У ролі конкретного прикладу можна назвати ситуацію, коли GuardDuty фіксує спробу EC2-інстансу встановити з'єднання з IP-адресою, якої раніше ніколи не бачив, і яка належить до вузлів TOR. Подібна мережева аномалія для цього інстансу породжує сповіщення, адже може свідчити про компрометацію й використання його для прихованої передачі даних. Без застосування МН такі відхилення, що враховують широкий контекст, були б надзвичайно складними для виявлення за наявності тисяч інстансів і з'єднань.

Автоматизоване реагування та усунення проблем. ШІ/МН не лише допомагають у виявленні проблем, а й у їхньому безпосередньому вирішенні. Одним з аспектів є прийняття інтелектуальних рішень у робочих процесах усунення проблем. Наприклад, як тільки CSPM ідентифікує некоректну конфігурацію, МН може допомогти визначити найкращу дію з усунення, навчаючись на минулих виправленнях. Окремі просунуті системи застосовують планування на базі ШІ, щоб безпечно пропонувати або навіть безпосередньо реалізовувати необхідні зміни.

На практиці багато рішень для хмарної безпеки інтегруються зі «serverless»-автоматизацією (наприклад, AWS Lambda чи Azure Functions) для автоматичного запуску дій у разі виявлення загроз. Тут ШІ визначає, коли саме слід ініціювати функцію й із якими параметрами. Скажімо, у Amazon GuardDuty можна налаштувати "automated response": якщо виявлено серйозну загрозу, GuardDuty може автоматично викликати Lambda-функцію для ізоляції інстансу, відкликання облікових даних або виконання інших термінових заходів. Рішення про запуск такої процедури може залежати від "рівня впевненості" (confidence score), розрахованого моделлю МН.

У розгорнутіших CNAPP-платформах на базі ШІ можливе оркестрування цілого ланцюжка реагування: якщо система виявляє кілька аномалій, що свідчать про триваючу атаку, вона здатна автоматично підвищувати пріоритет інциденту, обмежувати ризикові права доступу (якщо модуль CIEM визначає, що вони й так надмірні) та застосовувати політику ізоляції до скомпрометованих хмарних ресурсів. Крім того, набирає популярності аналітика прогнозного типу (predictive analytics), коли МН-моделі на основі історичних даних про атаки визначають, які вразливості найімовірніше будуть експлуатовані, і пропонують виправити їх насамперед (так звана "pre-emptive remediation"). У деяких дослідженнях описано "підхід на основі глибинного навчання до управління станом безпеки у хмарі", що дозволяє не лише виявляти проблеми, а й "проактивно визначати вразливості та некоректні налаштування, посилюючи захист хмарних середовищ" [7]. Такий підхід фактично дає змогу усувати вади, перш ніж зловмисники їх експлуатують.

Окремо варто згадати й про роль методів обробки природної мови (NLP) в аналізі журналів хмарного аудиту та архітектурної документації для виявлення можливих прогалин у безпеці й формування рекомендацій. З'являються також чат-боти чи віртуальні помічники на основі ШІ, що можуть аналізувати сповіщення й автоматично надавати аналітику з готовим планом усунення виявлених загроз, заощаджуючи час спеціалістів. Окрему перспективу становить застосування методів навчання з підкріпленням (reinforcement learning) у хмарній

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

авто-ремедіації: алгоритми поступово визначають найкращі дії реагування, взаємодіючи безпосередньо з оточенням. Хоча це поки на початковій стадії, однак такий підхід відкриває шлях до систем повністю автономного захисту хмари, які в реальному часі динамічно коригують налаштування для відбиття атак.

Водночас слід пам'ятати, що й самі моделі штучного інтелекту потребують управління: якісних даних для тренування, відстеження зміни їхньої точності й актуальності (особливо з огляду на еволюцію сценаріїв використання хмари та адаптації методів нападників). Але при правильній реалізації ШІ та МН довели, що значно покращують моніторинг стану безпеки хмарних середовищ. Вони ефективно вирішують проблему "голки в стозі сіна": просіюють величезні обсяги хмарних даних, щоб знайти слабкі сигнали ризику. У результаті команди безпеки виявляють загрози й конфігураційні вразливості швидше та точніше, ніж раніше.

Згідно з одним із досліджень, впровадження машинного навчання в моніторинг хмарної безпеки дозволило компанії Microsoft знизити кількість хибних сповіщень більш ніж на 50% і помітно прискорити реагування [13]. Також ШІ/МН відкриває можливості для формування моделей поведінки (behavior-based clustering) хмарних облікових записів, завдяки яким можна виявити, що певний акаунт раптом почав суттєво відхилятися від "типових" патернів колег і, ймовірно, був скомпрометований. Без методів машинного навчання такі глибокі аналізи були б надто складними в реалізації.

На практиці організації отримують вигоду від ШІ/МН завдяки функціям, вбудованим в інструменти хмарної безпеки: виявлення на основі МН в AWS GuardDuty, чи додатковими рішеннями від сторонніх розробників, які позиціонують ШІ як свою конкурентну перевагу (наприклад, метод "polygraph" від Lacework або використання ML у виявленні контейнерних загроз у CrowdStrike). Зі зростанням загроз ці моделі регулярно оновлюються новими знаннями (приміром, після аналізу великого витоку даних отримані патерни додаються в моделі, щоб розпізнавати схожі "copycat" атаки). Завдяки такій здатності "самонавчання" алгоритми стають дедалі результативнішими, а загальна безпека у хмарі — динамічною та адаптивною.

Синергія ШІ/МН з можливостями CSPM/CWPP/CNAPP в кінцевому підсумку призводить до більш автономної хмарної безпеки: середовище, яке може контролювати себе, виявляти аномалії і навіть певною мірою самовідновлюватися. Усе це дозволяє фахівцям зосередитися на стратегічних аспектах і безпосередньому реагуванні на критичні інциденти, делегуючи рутинні завдання автоматизованій інфраструктурі.

Висновки

Забезпечення надійного рівня безпеки у хмарних середовищах вимагає комплексного підходу. CSPM, CWPP та CNAPP поєднують різні "шари" хмарної інфраструктури:

- CSPM відповідає за безпеку та дотримання конфігурацій хмари;
- CWPP зосереджується на виявленні й блокуванні загроз безпосередньо у робочих навантаженнях;
- CNAPP об'єднує ці можливості в цілісне рішення, оптимізоване для хмарно-орієнтованих середовищ.

Кожний з підходів має свою "зону відповідальності" й уразливі місця, тому їхнє узгоджене використання дає змогу сформувати багатоетапну стратегію захисту (defense-in-depth). CSPM вирізняється ефективністю в попередженні та забезпеченні відповідності стандартам, CWPP – у виявленні загроз та реагуванні на них, тоді як CNAPP надає інтегрований підхід і підвищує загальну ефективність. Усі вони потребують належної конфігурації, розумного процесного забезпечення та доповнювальних механізмів контролю.

З огляду на динаміку та розподіленість хмар, надзвичайно важливою є автоматизація й залучення інтелектуальних алгоритмів. Технології на базі ШІ/МН стали "важелем" у цьому контексті, даючи змогу перетворювати колосальні масиви даних на корисну аналітику. Вони підсилюють ключові функції CSPM, CWPP та CNAPP за допомогою адаптивного,

© Скоринович Б.В., Лах Ю.В. (2025). Аналіз методів моніторингу стану безпеки в хмарному середовищі. Сучасний захист інформації, 1(61), 298–310.
https://doi.org/10.31673/2409-7292.2025.012256.

інтелектуального виявлення загроз та навіть пропонують заходи профілактики чи, у певних випадках, автоматичного усунення недоліків. Завдяки ефективному використанню ШІ/МН організації можуть суттєво підвищити здатність завчасно виявляти або принаймні швидко локалізувати інциденти.

Практично кажучи, компаніям, які прагнуть покращити свою хмарну безпеку, слід почати з впровадження CSPM як "базової лінії", що забезпечує безперервний моніторинг і коригування конфігурацій (це часто найшвидший спосіб знизити ризик витоків). Наступним кроком може бути використання CWPP для нагляду за критично важливими робочими навантаженнями та реагування на активні загрози (як через сервіси хмарного провайдера, так і за рахунок сторонніх рішень, які охоплюють різні типи ресурсів). По мірі зростання масштабів доцільно перейти до концепції CNAPP або повноцінної платформи, що спростить управління й уніфікує безпекові процеси в мультихмарному середовищі. Важливо також приділяти увагу підготовці фахівців: найкращі інструменти потребують належного налаштування і компетентної підтримки команд DevOps та безпеки.

Не менш значущим є організаційна складова: регулярні тренування сценаріїв реагування на інциденти, планові огляди безпекової пози й дотримання принципу "secure-by-design" на всіх етапах розгортання хмарних сервісів. У світлі швидкого розвитку тактик зловмисників і появи нових хмарних сервісів постійний моніторинг тенденцій і оновлення знань (через наукові публікації, звіти галузевих спільнот на кшталт NIST або Cloud Security Alliance та рекомендації провайдерів) стають критично важливими. Об'єднуючи правильні інструменти (CSPM, CWPP, CNAPP), задіюючи ШІ/МН і формуючи культуру безпеки, організації отримують змогу проактивно керувати ризиками та водночас користуватися перевагами гнучкості й інновацій, які пропонують хмарні платформи.

Перелік посилань

1. 2021 state of cloud security posture management report. Cloud Security Alliance. URL: https://cloudsecurityalliance.org/articles/2021-state-of-cloud-security-posture-management-report (дата звернення 20.12.2024).

2. Cloud misconfiguration. UpGuard. URL: https://www.upguard.com/blog/cloud-misconfiguration (дата звернення 21.12.2024).

3. Guffey, J., & Li, Y. (2023). Cloud service misconfigurations: Emerging threats, enterprise data breaches and solutions. In 2023 IEEE 13th Annual Computing and Communication Workshop and Conference (CCWC) (pp. 806–812). IEEE. https://doi.org/10.1109/CCWC57344.2023.10099296

4. Jimmy, F. (2023). Cloud security posture management: Tools and techniques. Journal of Knowledge Learning and Science Technology, 2(3). https://doi.org/10.60087/jklst.vol2.n3.p622

5. Coppola, G., Varde, A. S., & Shang, J. (2023). Enhancing cloud security posture for ubiquitous data access with a cybersecurity framework-based management tool. In 2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON) (pp. 590–594). IEEE. https://doi.org/10.1109/UEMCON59035.2023.10316003

6. What is CNAPP? Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-cnapp (дата звернення 15.01.2025).

7. Choubey, R. (2023). Machine Learning Algorithms for Cloud Computing Security: A Review. Tuijin Jishu/Journal of Propulsion Technology, 44(4), 7372–7375. https://doi.org/10.52783/tjjpt.v44.i4.2564

8. Proactively harden your cloud security posture in the age of AI with CSPM INNOVA. Microsoft Defender Cloud Blog. URL: https://techcommunity.microsoft.com/blog/MicrosoftDefenderCloudBlog/proactively-harden-your-cloud-security-posture-in-the-age-of-ai-with-cspm-innova/4297079 (дата звернення 15.01.2024).

9. GuardDuty features. Amazon Web Services. URL: https://aws.amazon.com/guardduty/features (дата звернення 01.10.2024).

10. Cloud security glossary. Cloud Security Alliance. URL: https://cloudsecurityalliance.org/cloud-security-glossary (дата звернення 15.01.2024).

11. What is CNAPP? Microsoft. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-cnapp (дата звернення 02.02.2024).

12. Vanitha, M., Navya Patel, M., Madhumitha, K., & Sathvika, J. (2024). Enhancing insider threat detection in cloud environments through ensemble learning. International Journal of Communication Networks and Information Security (IJCNIS), 16(5), 638–647. Retrieved from https://www.ijcnis.org/index.php/ijcnis/article/view/7870

Надійшла 27.02.2025