хмарних провайдерів варіюються від 30 секунд до декількох хвилин, що критично впливає на автоматичне зіставлення подій при розслідуванні крос-хмарних ланцюжків атак.

Висновки та практична значущість. Розроблена нормалізаційна схема на базі OCSF дозволяє скоротити кількість помилкових спрацювань автоматизованих playbooks на 34% у порівнянні з конфігурацією без нормалізації, що підтверджено тестовим розгортанням у лабораторному мультихмарному середовищі. Впровадження централізованого Identity Broker-шару для управління доступом між SOAR-платформою та API провайдерів скорочує час конфігурації нових інтеграцій у середньому на 60%.

Таблиця 1

Порівняння механізмів інтеграції SOAR з API хмарних провайдерів

Характеристика	AWS	Microsoft Azure	Google Cloud
Нативний SIEM/SOAR	Security Hub + GuardDuty	Microsoft Sentinel	Security Command Center
Формат подій	ASFF	Microsoft Graph Security API	CSCC API (JSON/gRPC)
Модель доступу	IAM Roles + STS	Service Principals (Entra ID)	Service Accounts + Workload Identity
Затримка телеметрії	~30–90 сек	~60–120 сек	~30–60 сек
Підтримка OCSF	Часткова (Preview)	Відсутня (власна схема)	Відсутня (власна схема)
Інтеграція SOAR (оцінка)	Висока	Висока	Середня

1. Flexera 2024 State of the Cloud Report. Flexera Software LLC, 2024. URL: https://www.flexera.com/blog/cloud/cloud-computing-trends-flexera-2024-state-of-the-cloud-report/
2. Kindervag J., McDonald K. Cloud-Native Security Guide: AWS, Azure, and GCP Security Services Comparison. Palo Alto Networks, 2023. 68 p.
3. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide. NIST Special Publication 800-61 Revision 2. NIST, 2012. 79 p.
4. Open Cybersecurity Schema Framework (OCSF) Specification v1.1. OCSF Project Contributors, 2023. URL: https://schema.ocsf.io/

AHP-підхід в управлінні інформаційною безпекою

УДК 004.056:519.816

Наталія Маслова[1,2], Р. Ткачук[1], Олена Любименко[2]

[1]Львівський державний університет безпеки життєдіяльності,
[2]Донецький національний технічний університет,
masgpp2@gmail.com, rlvtk@ukr.net, olena.liubymenko@donntu.edu.ua

У сучасних умовах цифрової трансформації та постійного зростання кількості кіберзагроз особливого значення набуває ефективне управління

інформаційною безпекою. Системи управління інформаційною безпекою потребують не лише впровадження технічних засобів захисту, а й застосування методів підтримки прийняття рішень, які дозволяють оцінювати альтернативні варіанти захисту інформації, визначати пріоритети безпеки та оптимізувати процес управління ризиками.

Одним із перспективних підходів до вирішення таких задач є застосування багатокритеріальних методів аналізу, зокрема методу аналізу ієрархій (Analytic Hierarchy Process, AHP), досвід застосування якого автори мали під час оцінювання характеристик інформаційних систем і web-застосунків [1].

Метою дослідження є аналіз можливостей використання методу AHP для підтримки прийняття рішень у системах управління інформаційною безпекою та оцінювання ефективності підходу до вибору механізмів захисту інформації.

У сфері інформаційної безпеки прийняття рішень потребує одночасного врахування технічних, організаційних та експлуатаційних факторів. За таких умов багатокритеріальний підхід дозволяє формалізувати процес вибору механізмів захисту інформації та визначати пріоритети безпеки з урахуванням сукупності критеріїв оцінювання. Метод аналізу ієрархій (AHP) забезпечує можливість поєднання кількісних і якісних показників та формування інтегральної оцінки альтернатив на основі експертного оцінювання. Однією з ключових задач управління інформаційною безпекою є вибір оптимальної моделі контролю доступу в умовах невизначеності та суперечливих вимог. Зокрема, необхідно враховувати рівень захищеності, масштабованість, складність адміністрування, відповідність нормативним вимогам і придатність до використання у хмарних та розподілених середовищах. Використання методу AHP дозволяє визначати відносну важливість критеріїв і виконувати комплексне оцінювання ефективності механізмів захисту інформації.

Метод аналізу ієрархій базується на побудові ієрархічної структури задачі, яка складається з трьох основних рівнів: мета прийняття рішення, критерії оцінювання, альтернативні варіанти [2, 3]. У межах методу AHP формується матриця попарного порівняння критеріїв, після чого обчислюються їх вагові коефіцієнти. Це дозволяє визначити найбільш важливі характеристики системи безпеки та сформувати інтегральну оцінку альтернатив. Як критерії оцінювання в системах управління інформаційною безпекою було використано рівень безпеки, гнучкість налаштування, складність адміністрування, масштабованість та придатність до використання у хмарних середовищах, для яких визначено відповідні вагові коефіцієнти.

Для демонстрації можливостей багатокритеріального підходу було проведено порівняльне оцінювання моделей контролю доступу із застосуванням методу AHP. У процесі оцінювання враховувалися критерії безпеки, масштабованості, гнучкості налаштування, складності адміністрування та придатності до використання у сучасних хмарних і розподілених середовищах (Таблиця 1).

За результатами багатокритеріального оцінювання моделей контролю доступу за методом AHP найбільш високі інтегральні пріоритети отримали моделі ABAC та Zero Trust Architecture. Це обумовлено їх підвищеною адаптивністю, можливістю врахування контекстних параметрів доступу та

кращою придатністю до використання у сучасних хмарних і розподілених інформаційних середовищах. Класичні моделі DAC і MAC отримали нижчі показники ефективності через обмежену гнучкість і складність масштабування.

Таблиця 1

Багатокритеріальне оцінювання моделей контролю доступу за методом AHP

Модель	Безпека	Масштабованість	Гнучкість	Складність адміністрування	Хмарна придатність	Інтегральний AHP-пріоритет
DAC	0,10	0,08	0,12	0,18	0,07	0,08
MAC	0,22	0,12	0,09	0,10	0,11	0,16
RBAC	0,20	0,21	0,18	0,19	0,17	0,22
ABAC	0,24	0,26	0,29	0,21	0,30	0,26
ZTA	0,24	0,33	0,32	0,32	0,35	0,28

Наукова новизна роботи полягає у застосуванні методу аналізу ієрархій для багатокритеріального оцінювання та вибору моделей контролю доступу в системах управління інформаційною безпекою з урахуванням технічних, організаційних та експлуатаційних критеріїв.

Отримані результати підтверджують доцільність застосування методу AHP для підтримки прийняття рішень у системах управління інформаційною безпекою. Метод аналізу ієрархій може використовуватися для оцінювання ефективності механізмів захисту інформації, вибору моделей контролю доступу та підтримки процесів управління ризиками в сучасних інформаційних системах.

1. Любименко О. М., Штепа О. А., Маслова Н. О., Стаценко О. А. Оцінювання якості web-застосунків управління проєктами на IT-ринку з використанням методу аналізу ієрархій // Науковий вісник Донецького національного технічного університету. 2026. с.99-106, https://doi.org/10.31474/2415-7902-2026-2-17-99-106
2. Saaty T. L. Decision Making with the Analytic Hierarchy Process // International Journal of Services Sciences. 2008. Vol. 1. No. 1. P. 83–98.
3. Sandhu R., Coyne E., Feinstein H., Youman C. Role-Based Access Control Models // IEEE Computer. 1996. Vol. 29. No. 2. P. 38–47.

Використання автоенкодерів для виявлення кібербезпекових аномалій в інформаційно-телекомунікаційних мережах

УДК 004.056:004.8

Євгенія Іванченко[1], Микола Рижаков[2],
Євген Кихтенко[3], Артем Роженко[4]

Державний університет інформаційно-комунікаційних технологій,
[1]e.ivanchenko@duikt.edu.ua, [2]m.ryzhakov@duikt.edu.ua,
[3]e.kykhtenko@stud.duikt.edu.ua, [4]a.rozhenko@stud.duikt.edu.ua

Об'єкти критичної інфраструктури держави — енергетика, транспорт, водопостачання, фінансовий сектор, телекомунікації, охорона здоров'я та