КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.32.1191
УДК 004.75; 004.8

Марценюк Євгеній Віталійович
аспірант кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID: 0009-0009-2289-0968
yevhenii.v.martseniuk@lpnu.ua

Дейнека Олег Романович
аспірант кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID: 0009-0005-9156-3339
deinekaoleg.86@gmail.com

Гарасимчук Олег Ігорович
к.т.н., доцент доцент кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID: 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

Луковський Тарас Ігорович
к.т.н., доцент кафедри захисту інформації
Національний Університет "Львівська Політехніка", Львів, Україна
ORCID: 0009-0008-1652-8121
taras.i.lukovskyi@lpnu.ua

ІНТЕГРАЦІЯ FINOPS ТА КОНТРОЛІВ SOC 2 У СИСТЕМІ БЕЗПЕКИ МУЛЬТИХМАРНИХ СЕРЕДОВИЩ

Анотація. Проблема забезпечення прозорості витрат і проактивного контролю бюджету в мультихмарних середовищах стає дедалі актуальнішою для сучасних IT-інфраструктур. Оскільки організації масштабують використання гетерогенних хмарних сервісів, вони постають перед викликами, пов'язаними з фрагментарністю платіжних систем, неузгодженістю метрик витрат і затримками у виявленні аномалій. У цьому дослідженні спостережність за витратами (cost observability) розглядається не просто як фінансова функція, а як невід'ємний компонент стратегії безпеки організації, узгоджений із фреймворком SOC 2. Наукова новизна роботи полягає в інтеграції інструментів моніторингу витрат – зокрема Splunk, Cherwell та хмарних API на базі JSON – з операційними процесами та процесами безпеки. Це дозволяє в реальному часі виявляти відхилення від бюджету, автоматизувати ескалацію інцидентів та впроваджувати політики контролю на основі фінансових показників.

У дослідженні представлено архітектуру майбутнього, яка впроваджує уніфікований рівень спостережності за витратами в гетерогенних білінгових системах мультихмарних середовищ. Архітектура трансформує специфічні формати провайдерів – включаючи JSON-експорти AWS Cost Explorer, API Azure Cost Management та експорти GCP Billing у BigQuery – у стандартизовані події витрат. Ці нормалізовані потоки формують єдину часову шкалу видатків відносно уніфікованих бюджетних порогів, одночасно генеруючи консолідовану фінансову телеметрію для міжпровайдерного виявлення аномалій та кореляції даних.

Завдяки переосмисленню фінансових даних як дієвих сигналів спостережності, цей підхід дозволяє перейти від фрагментованих дашбордів до централізованого, готового до аудиту рівня управління, що підтримує відповідність, реагування на інциденти та фінансовий менеджмент. Система також включає логіку доступу на основі ролей (RBAC), пороги ескалації та моделі прогнозування, створюючи рівень управління витратами, що має пряме значення для команд FinOps, DevSecOps та Compliance.

Ключові слова: мультихмарна інфраструктура, SOC2, хмарна безпека, моніторинг витрат, оптимізація бюджету, FinOps, автоматизація сповіщень, прогнозування витрат, Splunk, хмарна оркестрація, управління витратами, хмарне врядування (cloud governance).

ВСТУП

Сучасні IT-організації все частіше постають перед викликами щодо підтримки прозорості витрат та послідовного фінансового врядування у роботі з кількома хмарними провайдерами. Відмінності в моделях виставлення рахунків, структурах даних та механізмах звітності призводять до фрагментарної видимості, затримок у виявленні аномалій та обмежених можливостей для аудиту.

Проблематика дослідження: Це дослідження представляє запропоновану уніфіковану архітектуру спостережності за витратами, яка консолідує фінансові та операційні дані в єдине представлення, доступне для запитів. Система трансформує розрізнені потоки білінгу від AWS, Azure та GCP у стандартизовані події витрат, що дозволяє проводити уніфікований аналіз та кореляцію аномалій між різними провайдерами. Такий підхід змінює парадигму від ізольованих дашбордів до централізованого рівня спостережності, який інтегрує робочі процеси бюджетування, моніторингу та відповідності в межах спільної структури, узгодженої з SOC 2 Type II. Це забезпечує підзвітність на основі ролей, логіку ескалації та механізми прогнозування, що розширюють фінансову спостережність до загальної стратегії безпеки організації.

Така інтеграція є особливо актуальною в контексті відповідності зовнішнім стандартам інформаційної безпеки, зокрема SOC (Service Organization Control) 2. Ці стандарти вимагають впровадження процедур контролю в таких категоріях, як безпека, доступність та цілісність обробки (TSC). У зв’язку з цим моніторинг витрат розглядається не лише як інструмент фінансової оптимізації, а й як частина моделі операційної безпеки, де фінансові аномалії можуть слугувати індикаторами ризику, а сама система надає докази для аудитів.

Мета роботи: Основною метою цього дослідження є розробка та обґрунтування архітектурного рішення для моніторингу витрат у мультихмарному середовищі, яке не лише реалізує принципи фінансових операцій (FinOps), а й забезпечує відповідність критеріям інформаційної безпеки згідно з вимогами SOC 2. Такий підхід дозволяє інтегрувати технічний, фінансовий та аудиторський контроль у межах єдиної системи, спрямованої на підвищення прозорості, керованості та довіри до хмарної інфраструктури.

Використовуючи наочний приклад із реальної практики, у роботі аналізується процес побудови такої системи, її компоненти інтеграції, логіка ескалації та ролі зацікавлених сторін. Крім того, представлено огляд сучасних академічних досліджень, зосереджених на фінансовому моніторингу в хмарних середовищах, зокрема в контексті FinOps та Cloud Cost Governance (управління витратами у хмарі).

Нотація та термінологія. Цей підрозділ визначає акроніми, ролі та математичні символи, що використовуються в роботі, для забезпечення чіткості та послідовності викладу.

Акроніми:

- SOC 2 – Service Organization Control 2 (Контроль сервісних організацій 2);
- TSC – Trust Services Criteria (Критерії довірчих послуг);
- FinOps – Financial Operations (Фінансові операції);

- CMDB – Configuration Management Database (База даних керування конфігураціями);
- SIEM – Security Information and Event Management (Управління інформацією та подіями безпеки);
- ITSM – IT Service Management (Управління IT-сервісами);
- CSA – Cloud Service Allocation (Розподіл хмарних сервісів).

Позначення ролей:

- Власник бюджету (Budget Owner) – особа, відповідальна за витрати на рівні проєкту.
- Власник CSA (CSA Owner) – відповідальний за розподіл хмарних сервісів із повноваженнями на рівні кількох проєктів.
- Менеджер проєкту (Project Manager) – технічний керівник, відповідальний за управління робочими навантаженнями.

Математичні символи:

- C(t): фактичні накопичені витрати на момент часу t.
- B: затверджений бюджет.
- θ_k: попередньо визначений поріг витрат (наприклад, 0.7, 0.9, 1.0).
- α: темп зростання витрат.
- β: початкові накопичені витрати на початку розрахункового періоду.
- t_k^*: розрахунковий час досягнення порогу θ_k.

Об’єктом дослідження є мультихмарна IT-інфраструктура організації та процеси управління і моніторингу хмарних витрат у її межах з позиції забезпечення інформаційної безпеки та відповідності стандарту SOC 2. Дослідження зосереджується на функціонуванні системи фінансового контролю в гетерогенному хмарному середовищі, де дані про витрати інтегруються з операційними та безпековими процесами організації.

ОСНОВНА ЧАСТИНА

Методологія. Для досягнення поставленої мети в цьому дослідженні застосовується практико-орієнтована методологія архітектурних досліджень, заснована на аналізі реальних сценаріїв та операційних даних. Методологічний підхід починається з розробки прикладної архітектури системи, що інтегрує визнані технологічні компоненти. Зокрема, рішення використовує Splunk для агрегації даних та аналітики витрат, Cherwell як платформу для управління інцидентами та запитами, а також нативні білінгові API основних хмарних провайдерів (AWS, Azure, GCP) для збору даних про витрати в режимі близькому до реального часу.

Дослідження також включає сценарійний аналіз, який вивчає практичні випадки використання, пов'язані з порушенням фінансових порогів, автоматизованим сповіщенням та логікою ескалації, розподіленою між декількома організаційними ролями. Особлива увага приділяється конфігурації порогів споживання бюджету, часу реагування системи та механізмам сповіщення на основі ролей, що відображає реальну операційну практику.

Для оцінки відповідності запропонованої системи визнаним стандартам безпеки, впроваджена архітектура зіставлена з критеріями SOC 2 TSC. Це зіставлення визначає, як конкретні події, пов'язані з витратами (такі як неочікуване перевищення бюджету або відхилення від прогнозного споживання), можуть слугувати операційними

тригерами в робочих процесах безпеки та відповідності, зокрема тих, що стосуються цілісності обробки, доступності та моніторингу.

Методологічна база також включає огляд відповідної академічної та галузевої літератури, зосереджений на сучасних підходах до управління витратами у хмарі, еволюції практик FinOps та механізмах відповідності в розподілених хмарних середовищах. Цей теоретичний фундамент підкріплює обґрунтування того, що спостережність за витратами є формою операційного контролю.

Нарешті, ефективність запропонованої моделі підтверджується шляхом ретроспективного аналізу історичних даних білінгу. Цей етап передбачає вивчення змін у ключових показниках – таких як дотримання бюджету, час ескалації та фінансова прозорість – після впровадження системи. Результати цієї емпіричної оцінки формують висновки щодо практичного впливу та можливості реплікації підходу в мультихмарних інфраструктурах корпоративного масштабу.

Підтвердження цієї гіпотези дозволяє розглядати мультихмарну інфраструктуру не просто як технічне рішення, а як кероване середовище, в якому прозорість витрат і контроль стають критичними факторами сталого розвитку, фінансової стабільності та відповідності зовнішнім аудиторським стандартам.

Огляд літератури. Питання моніторингу та оптимізації витрат у мультихмарних середовищах активно досліджується в сучасній науковій літературі, особливо в контексті зростаючої складності управління фінансовими ресурсами на гетерогенних хмарних платформах. Протягом останніх років вектор досліджень змістився від суто технічних аспектів управління інфраструктурою до інтегрованих підходів, що поєднують обчислювальні ресурси, аналітику витрат та практики фінансового менеджменту.

У роботі Alexander та ін. (2020) [1] запропоновано модель оркестрації, що враховує витрати (cost-aware orchestration model). Вона інтегрує стандарт TOSCA з кастомною політикою оцінки та прогнозування витрат. Автори стверджують, що врахування майбутніх витрат під час оркестрації не лише забезпечує гнучке масштабування додатків, а й допомагає утримувати видатки в межах допустимих бюджетних лімітів. Це є значним кроком до побудови динамічних, саморегульованих систем фінансового контролю в мультихмарних середовищах.

Вітчизняні дослідження, зокрема стаття Шокотько та ін. (2024) [2], розглядають трифазний підхід до управління хмарними витратами, який включає розуміння факторів витрат, контроль бюджетів та оптимізацію видатків. Автори наголошують на важливості впровадження практик FinOps для підвищення фінансової прозорості та рекомендують використовувати вбудовані інструменти хмарних провайдерів для щоденного моніторингу.

Проблема вибору оптимального хмарного провайдера на основі вартості виконання запитів розглядається у дослідженні Wojtowicz та ін. (2022) [3]. Запропонована модель дозволяє формувати оптимальний план запитів на основі вартості та продуктивності, що є вкрай актуальним для компаній, які працюють із великими обсягами даних у мультихмарних середовищах. Цей підхід підкреслює необхідність глибшої інтеграції моніторингу витрат на рівні аналітичних запитів та систем управління даними.

Дослідження Fang Li та ін. (2022) [4] зосереджено на практичній реалізації платформи SmartCMP, яка автоматизує моніторинг витрат і забезпечує централізоване управління політиками оптимізації в мультихмарних середовищах. Платформа

дозволяє встановлювати бюджети, виявляти аномалії та ініціювати дії для зменшення перевитрат, що демонструє практичну ефективність підходів FinOps.

Окремої уваги заслуговує дослідження Thumala & Pillai (2024) [5], присвячене оптимізації витрат під час міграції у хмару. Автори описують методології підбору оптимальних потужностей (rightsizing), управління зарезервованими інстансами, оптимізацію мережевої взаємодії між хмарами та оцінюють ефективність різних фінансових стратегій залежно від типу навантаження. Це підтверджує необхідність багаторівневого підходу до управління витратами, що включає як інженерні, так і фінансові рішення.

Підсумовуючи, наукова література підтверджує, що ефективне управління витратами в мультихмарному середовищі вимагає:

- Використання підходів динамічного моделювання витрат;
- Впровадження інтегрованих платформ для збору та аналізу фінансових даних;
- Застосування практик FinOps та врядування (governance) для узгодження роботи IT-відділів та фінансових команд;
- Прогнозування витрат та своєчасного реагування на аномалії за допомогою автоматизованих сповіщень та управління інцидентами.

У сучасному цифровому ландшафті, де хмарні технології є основою для масштабованих, гнучких та високонадійних IT-рішень, моніторинг витрат набуває стратегічного значення. Зростаюча популярність мультихмарних архітектур, що передбачають одночасне використання сервісів від різних хмарних провайдерів, посилює потребу в прозорості витрат, прогнозуванні фінансових ризиків та ефективному управлінні бюджетом [5].

Розглянуті наукові джерела чітко вказують на те, що ефективний моніторинг витрат – це не лише інструмент фінансового контролю, а й ключовий фактор забезпечення стабільності та передбачуваності IT-сервісів. Зокрема, поєднання інструментів моніторингу (Splunk, SmartCMP), автоматизованого реагування на перевитрати, практик FinOps та інтеграції з рішеннями CMDB (наприклад, Cherwell) дозволяє організаціям приймати обґрунтовані управлінські рішення на основі реальних даних.

Таким чином, моніторинг витрат у мультихмарному середовищі еволюціонує з допоміжної функції у критично важливий компонент хмарного врядування (cloud governance), що забезпечує баланс між технічною ефективністю та фінансовою підзвітністю. Це підкреслює необхідність подальших досліджень та розгортання систем, які інтегрують технічну аналітику, бізнес-логіку та автоматизоване реагування для забезпечення сталого функціонування сучасних IT-екосистем [6].

Роль FinOps у моніторингу витрат у мультихмарній інфраструктурі. FinOps став методологічною основою для прозорого та підзвітного використання хмарних ресурсів у мультихмарних середовищах. Знаходячись на перетині фінансів, розробки та операційної діяльності, він забезпечує уніфіковану структуру, де зацікавлені сторони мають спільне розуміння обсягів витрат, механізмів контролю та практик оптимізації витрат [7].

У мультихмарних умовах, де моделі білінгу відрізняються, а відстеження витрат є фрагментарним, FinOps дозволяє нормалізувати бюджетні метрики між провайдерами (AWS, Azure, GCP) та узгодити витрати з бізнес-цілями. У межах запропонованої архітектури принципи FinOps реалізуються через агрегацію витрат і порівняння з бюджетом у Splunk, автоматизоване виявлення порогів, ескалацію через Cherwell із

розподілом ролей між командами DevSecOps і SecOps, а також щомісячне прогнозування за допомогою дашбордів Splunk.

Таким чином, FinOps не обмежується інструментами, а функціонує як концептуальна основа, що пов'язує фінансові метрики з технічними подіями та організаційною відповідальністю. Важливо, що він також підтримує критерії SOC 2 – зокрема Цілісність обробки та Безпеку – гарантуючи, що аномалії витрат розглядаються як частина ширшого середовища контролю організації [8].

SOC 2 як захід безпеки для хмарних витрат. У контексті управління мультихмарною інфраструктурою все більше організацій прагнуть забезпечити не лише технічну ефективність використання ресурсів, а й відповідність вимогам безпеки, прозорості та підзвітності. Одним із найбільш широко впроваджуваних фреймворків, що формалізує ці вимоги, є SOC 2 – система контролю, розроблена Американським інститутом сертифікованих публічних бухгалтерів (AICPA) для оцінки ефективності інформаційної безпеки в організаціях, що надають хмарні та технологічні послуги.

SOC 2 базується на TSC – принципах, що визначають очікувану поведінку організації у сферах Безпеки, Доступності, Цілісності обробки, Конфіденційності та Приватності.

Звіти SOC 2 складаються згідно зі Стандартом атестаційних завдань № 18 (SSAE-18), який є основою для оцінки дизайну та ефективності заходів контролю. Існує два типи звітів SOC 2: Тип I, який оцінює дизайн контролів у певний момент часу, та Тип II, який оцінює операційну ефективність цих контролів протягом визначеного періоду спостереження. Оскільки це дослідження розглядає моніторинг витрат як безперервний операційний процес, аналіз узгоджується насамперед із SOC 2 Тип II. Обговорення зосереджене на TSC, найбільш релевантних для фінансової спостережності та реагування на ризики в мультихмарних середовищах – зокрема Безпеці, Доступності, Цілісності обробки та Моніторинговій діяльності. Таке узгодження підкреслює здатність системи демонструвати ефективність контролю протягом тривалого часу, а не лише адекватність самого дизайну.

У межах цієї структури моніторинг витрат може бути операціоналізований як захід контролю SOC 2 Типу II, що підтримує відповідність та пом'якшення ризиків у мультихмарних середовищах [9].

Моніторинг витрат із оповіщеннями на основі порогів, ескалацією інцидентів та історією реагування може розглядатися як контрольна діяльність, що забезпечує:

- Виявлення відхилень від очікуваної поведінки системи, які можуть бути результатом несанкціонованого або неналежного використання ресурсів;
- Перевірку належного функціонування IT-процесів (наприклад, автоматичне відключення зайвих інстансів або реакція на перевищення бюджету);
- Реєстрацію подій для цілей аудиту, включаючи збір логів у системах SIEM або сервісах на кшталт Splunk;
- Розподіл ролей і обов'язків (CSA, FinOps, DevSecOps) згідно з політиками управління доступом, що є частиною вимог SOC 2 до підзвітності.

Інтеграція моніторингу витрат із такими системами, як Cherwell, ServiceNow та Splunk, дозволяє впровадити багаторівневу модель реагування, де кожна фінансова подія розглядається як потенційна бізнес-подія або подія безпеки. Це відповідає процедурним вимогам SOC 2 Типу II, де критично важливою є послідовність процесів у часі [10]. Таким чином, моніторинг витрат у мультихмарному середовищі може не лише оптимізувати фінансове споживання, а й слугувати операційним контролем у межах фреймворку SOC 2. Цей підхід поєднує FinOps та інформаційну безпеку,

створюючи основу для всебічної відповідності та підвищення довіри з боку клієнтів, партнерів та аудиторів.

Зрештою, включення моніторингу хмарних витрат як частини стратегії безпеки організації сприяє загальному зміцненню безпеки. Фінансові аномалії часто відображають глибші операційні проблеми або проблеми з конфігурацією – такі як неправильно розподілені ресурси, несанкціоноване розгортання або порушення політик – які можуть бути не відразу помітними лише через традиційний технічний моніторинг. Розглядаючи неочікувані витрати як потенційний індикатор ризику, організації отримують додатковий вимір ситуаційної обізнаності, що посилює як превентивні, так і детективні заходи контролю.

Таким чином, нагляд за хмарними витратами стає значущим розширенням операцій з безпеки організації. Він додає рівень бізнес-орієнтованої видимості технічним середовищам, зміцнює механізми підзвітності та підтримує раннє виявлення поведінки, що може вказувати на злами, зловживання або порушення відповідності. Отже, інтеграція моніторингу хмарних витрат у структури безпеки, узгоджені з SOC 2, не лише задовольняє очікування аудиту, але й покращує здатність організації керувати ризиками проактивно та цілісно.

Зіставлення з TSC SOC 2 та модель ризиків. Фреймворк зіставлення встановлює зв'язок між засобами контролю системи та критеріями TSC, що є найбільш релевантними для мінімізації ризиків безпеки. Використана модель ризиків адаптована з посібника NIST SP 800-30 «Guide for Conducting Risk Assessments», що забезпечує структурований та стандартизований підхід до ідентифікації загроз, оцінки ймовірності та аналізу впливу. Функції моніторингу витрат розглядаються з погляду їхнього внеску у зменшення конкретних сценаріїв загроз, де фінансові аномалії виступають як вторинні індикатори операційних подій або подій безпеки.

Для кожного ідентифікованого сценарію загрози було оцінено як ймовірність виникнення, так і потенційний вплив на критерії SOC 2 – зокрема на Безпеку, Доступність та Цілісність обробки. Основними розглянутими загрозами є:

- Несанкціоноване надання ресурсів – свідчить про скомпрометований доступ або обхід контролю змін.
- Необліковані або «тіньові» робочі навантаження – призводять до неконтрольованих витрат і порушення відповідності політиці.
- Вичерпання бюджету – призводить до потенційних перебоїв у обслуговуванні та порушення зобов'язань щодо доступності.
- Неефективна конфігурація сповіщень – затримує виявлення та реагування на аномальну діяльність.
- Зловживання ресурсами – спричиняє фінансові втрати та ризики регуляторного впливу.

Ідентифіковані сценарії ризиків зіставлені з TSC SOC 2, щоб продемонструвати чітке охоплення відповідності, яке забезпечується впровадженими засобами контролю. Це зіставлення пов'язує кожен релевантний критерій із конкретним технічним заходом у системі моніторингу витрат і визначає відповідний мінімізований ризик. Основна увага приділяється критеріям, безпосередньо пов'язаним із безпекою, доступністю та цілісністю обробки, що відображає, як фінансова спостережність підтримує як превентивні, так і детективні засоби контролю в мультихмарних середовищах.

Таблиця 1

Зіставлення TSC SOC 2 із впровадженими засобами контролю та мінімізованими ризиками

Критерій SOC 2 Trust Services	Впроваджений у системі захід контролю	Мінімізований ризик
CC6.1 Логічний захист доступу	Керування доступом на основі ролей (RBAC) у Splunk та Cherwell; обмеження змін параметрів бюджету	**Несанкціоноване надання ресурсів** – запобігання змінам з боку неуповноваженого персоналу
CC6.6 Розподіл обов'язків	Розмежування відповідальності між FinOps, DevSecOps та SecOps щодо схвалення змін та вирішення інцидентів	**Несанкціоноване надання ресурсів** – мінімізація ризиків від скомпрометованих облікових записів або обходу процесів схвалення
CC7.2 Виявлення та моніторинг компонентів системи	Автоматичне виявлення немаркованих (untagged) або несанкціонованих робочих навантажень через патерни аномалій витрат	**Необліковані або «тіньові» навантаження** – ідентифікація неконтрольованих ресурсів та пов'язаних із ними видатків
A1.2 Зобов'язання щодо доступності	Процеси ескалації при ризику вичерпання бюджетних порогів; пріоритезація критично важливих навантажень	**Вичерпання бюджету** – запобігання перебоям у роботі сервісів та порушенням угод про рівень послуг (SLA)
CC7.3 Реагування на інциденти	Сповіщення на основі порогів у Splunk, автоматична ескалація через Cherwell/ServiceNow	**Неефективна конфігурація сповіщень** – забезпечення своєчасного виявлення та реагування на аномальну активність витрат
PI1.1 Цілісність обробки	Регулярне отримання та валідація даних про витрати через API AWS, Azure та GCP	**Неефективна конфігурація сповіщень** – запобігання помилково негативним результатам через неповні або неточні дані
CC7.4 Реєстрація та моніторинг діяльності	Централізоване логування випадків порушення бюджету, ескалацій та результатів їх вирішення у Splunk	**Зловживання ресурсами** – створення аудиторського сліду для виявлення та розслідування несанкціонованого використання
CC9.2 Конфіденційність інформації	Контрольований доступ до фінансових звітів та даних про розподіл витрат	**Зловживання ресурсами** – обмеження доступу до чутливих фінансових даних, які можуть бути використані для експлуатації

Це зіставлення ілюструє, що функції спостережності за фінансами виходять за межі управління бюджетом, формуючи невід'ємну частину середовища контролю безпеки організації. Шляхом узгодження механізмів моніторингу витрат із TSC SOC 2, система забезпечує раннє виявлення аномальної діяльності, впроваджує підзвітність на основі ролей та зберігає готові до аудиту докази обробки інцидентів. Отже, нагляд за хмарними витратами стає як інструментом забезпечення відповідності, так і засобом проактивного пом'якшення ризиків, зміцнюючи загальну стійкість і надійність мультихмарних операцій.

Огляд IT-рішень для моніторингу хмарних витрат. Управління витратами в хмарних середовищах – це не лише зменшення рахунків; це насамперед забезпечення прозорості, передбачуваності та фінансової дисципліни в умовах динамічного споживання ресурсів. Із зростанням складності мультихмарної інфраструктури організації постають перед новими викликами: неузгодженість форматів звітності між провайдерами, відмінності в моделях ціноутворення, затримки в оновленні даних та недостатня інтеграція фінансових інструментів із технічною інфраструктурою [11].

У цьому контексті зростає важливість як методологічно обґрунтованого аналітичного підходу, так і вибору відповідних IT-рішень, здатних підтримувати повний цикл моніторингу – від збору даних до автоматизованого реагування. Побудова ефективної системи контролю витрат потребує врахування не лише технічних аспектів збору метрик, а й організаційних процесів, пов'язаних із бюджетуванням, аналітикою та міжвідомчою взаємодією.

Більшість постачальників хмарних послуг – таких як Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP) – пропонують власні сервіси для моніторингу та контролю витрат. Ці сервіси розроблені для надання як базових, так і розширених інструментів для аналізу витрат, планування бюджету та сповіщення про перевищення фінансових порогів [12].

Вбудовані сервіси моніторингу витрат від хмарних провайдерів. Хмарні провайдери першого ешелону – AWS, Azure та GCP – пропонують власні інструменти для відстеження та контролю витрат. Такі сервіси, як AWS Cost Explorer, Azure Cost Management та Google Cloud Billing Reports, забезпечують базову аналітику, створення бюджетів, налаштування сповіщень про порушення порогів та генерацію звітів.

Ці інструменти дозволяють користувачам візуалізувати дані в реальному часі, створювати прогнози та впроваджувати початковий рівень фінансового контролю, не покладаючись на зовнішні рішення. Однак їх використання обмежене інфраструктурою лише одного провайдера, що унеможливлює комплексний контроль у мультихмарному середовищі. Тому вбудовані сервіси часто використовуються як основа для подальшої інтеграції з незалежними платформами класу FinOps [13].

AWS: Cost Explorer та AWS Budgets. AWS Cost Explorer – це візуальний інструмент, який дозволяє аналізувати хмарні витрати за допомогою діаграм і таблиць. Він дає змогу користувачам:

- Переглядати витрати щоденно, щомісячно або за обраний період.
- Групувати витрати за сервісами (EC2, S3, RDS тощо), тегами та акаунтами.
- Виявляти аномалії або неочікуване зростання витрат.
- Аналізувати тенденції витрат для прогнозування.

Сервіс AWS Budgets дозволяє встановлювати індивідуальні ліміти бюджету для конкретних акаунтів, хмарних сервісів, проєктів або ресурсів із визначеними тегами. При досягненні встановленого порогу витрат (наприклад, 80% від заданого бюджету) система автоматично генерує сповіщення, які можуть бути надіслані електронною поштою або через сервіс повідомлень Amazon SNS. Ці сервіси інтегровані в AWS Billing Dashboard і є безкоштовними (деякі розширені функції аналітики можуть бути платними при великих обсягах даних) [14].

Microsoft Azure: Cost Management + Billing. Azure Cost Management + Billing - це комплексний набір інструментів для моніторингу, аналізу та оптимізації витрат у хмарному середовищі Microsoft Azure. Система забезпечує детальну візуалізацію фінансових метрик за підписками, групами ресурсів, окремими ресурсами, тегами та конкретними періодами часу. Однією з ключових особливостей є автоматична генерація звітів про бюджет із можливістю їх розсилки визначеним одержувачам.

Цей сервіс є особливо зручним для великих організацій, які активно використовують Office 365 або Power Platform, оскільки він добре інтегрується з іншими інструментами Microsoft [15].

Google Cloud Platform: Billing Reports та Budgets. Google Cloud Billing Reports - це візуальний інтерфейс, призначений для аналізу витрат на хмару в екосистемі Google Cloud. Інструмент забезпечує детальну аналітику за проєктами, акаунтами, окремими

сервісами та географічними регіонами. Ключові функції включають побудову графіків витрат на основі різних параметрів, порівняння поточних фінансових метрик із даними за попередні періоди та ідентифікацію сервісів чи проєктів, що генерують найбільші витрати.

Крім того, Google BigQuery Billing Export дозволяє експортувати детальні дані білінгу в BigQuery, де за допомогою SQL-запитів можна будувати гнучку аналітику витрат, створювати звіти та виконувати кастомне прогнозування витрат [16].

Обмеження вбудованих сервісів. Попри значну функціональність і простоту використання, вбудовані сервіси моніторингу витрат від хмарних вендорів (AWS, Azure, GCP) мають низку фундаментальних обмежень, які знижують їхню ефективність у складних мультихмарних сценаріях.

По-перше, ці сервіси тісно прив'язані до екосистеми одного провайдера, що унеможливлює створення консолідованого представлення витрат у середовищах, де використовуються кілька хмарних платформ. Відсутність кросплатформеної сумісності обмежує можливості централізованого фінансового моніторингу та ускладнює впровадження підходу FinOps у мультихмарному контексті.

По-друге, спостерігається відсутність уніфікованої логіки білінгу та звітності через різницю у форматах представлення витрат, частоті оновлення даних та рівнях деталізації. Це ускладнює порівняльний аналіз та інтеграцію даних із різних джерел. Третім обмеженням є базовий рівень автоматизації. Хоча ці інструменти можна інтегрувати з такими сервісами, як AWS Lambda, Microsoft Power Automate або Google Pub/Sub, це все одно потребує додаткової розробки. Крім того, стандартний функціонал не охоплює складні сценарії ескалації, багаторівневу взаємодію команд або адаптацію до внутрішніх організаційних політик.

Нарешті, вбудовані сервіси пропонують обмежену підтримку бізнес-контексту, оскільки вони зосереджені переважно на технічних параметрах ресурсів. Це ускладнює зіставлення витрат з організаційними структурами (департаментами, командами, клієнтами), бізнес-процесами або ключовими показниками ефективності (KPI), які є критично важливими для стратегічного фінансового менеджменту [17].

Вбудовані сервіси моніторингу витрат є першим кроком до контролю хмарних бюджетів. Вони добре підходять для компаній, які використовують одного провайдера і хочуть встановити базові правила контролю, оповіщення та аналітики. Проте у випадку мультихмарної стратегії або необхідності централізованого підходу FinOps цих інструментів зазвичай недостатньо. У таких ситуаціях на допомогу приходять незалежні мультихмарні рішення, що пропонують комплексну інтеграцію, гнучкіші правила, автоматизацію та фінансову аналітику [18].

Незалежні мультихмарні платформи для моніторингу витрат. Ці платформи реалізують принципи FinOps, представлені в Розділі 2, забезпечуючи агрегацію витрат, оповіщення на основі порогів та автоматизовану ескалацію.

Apptio Cloudability. Провідна FinOps-платформа для агрегації, аналізу та оптимізації витрат у AWS, Azure, GCP, Kubernetes [19] та локальній (on-premises) інфраструктурі. Вона пропонує візуалізацію витрат за проєктами, командами та сервісами; прогнозування видатків та рекомендації з оптимізації (наприклад, перехід на Reserved або Spot інстанси). Підтримує контроль лімітів бюджету, дашборди, автоматизовану звітність та адаптивні звіти на основі ролей для фінансових, технічних та DevOps команд [20].

Flexera One (раніше RightScale). Платформа корпоративного рівня, що поєднує можливості CMDB із моніторингом витрат та впровадженням політик для хмарних і

локальних ресурсів. Вона дозволяє деталізувати витрати, проводити бенчмаркінг та виявляти неефективне використання з автоматизацією дій для економії. Інтеграція з інструментами ITSM (наприклад, ServiceNow, Cherwell) підтримує автоматизовану обробку інцидентів та схвалення робочих процесів, що робить її вдалим вибором для великих складних організацій [21].

Spot by NetApp. Платформа, зосереджена на автоматизованій оптимізації хмарних ресурсів у реальному часі для максимальної економічної ефективності при збереженні продуктивності сервісів. Вона автоматизує перемикання між типами обчислювальних інстансів, динамічно масштабує кластери Kubernetes (через Ocean) та надає рекомендації щодо зниження витрат – ідеально для команд DevOps та SRE у високодинамічних середовищах [22].

CloudHealth by VMware. Платформа фінансового управління хмарою, що використовується великими підприємствами та постачальниками керованих послуг (MSP). Вона агрегує білінгові та операційні дані з основних хмар, візуалізує витрати та KPI, підтримує рольовий доступ, інтегрується з інструментами відповідності та будує фінансові моделі для прийняття стратегічних рішень щодо розгортання в AWS, Azure та GCP [23].

Порівняння мультихмарних платформ для моніторингу витрат. Проведений огляд та порівняльний аналіз незалежних мультихмарних платформ для моніторингу витрат демонструє (Таблиця 2), що сучасний ринок пропонує гнучкі та функціонально багаті рішення для впровадження стратегії FinOps в IT-організаціях.

Таблиця 2

Платформа	Підтримка мультихмарності	Автоматизація	Інтеграція з ITSM/ CMDB	Прогнозу-вання витрат	Функції безпеки
Apptio Cloudability	AWS, Azure, GCP, Kubernetes, On-Prem	Так (рекомендації, підбір потужностей (rights-sizing), зобов'язання)	Опосередковано	Так	Керування доступом на основі ролей (RBAC), шифроване зберігання даних, підтримка узгодження з SOC 2
Flexera One	AWS, Azure, GCP, On-Prem	Так (виявлення перевитрат, політики)	Так (наприклад, ServiceNow)	Так	Потужне управління політиками, інтеграція з CMDB, врядування доступом
Spot by NetApp	AWS, Azure, GCP, Kubernetes	Так (автооптимізація Spot/Reserved, Kubernetes)	Ні	Ні	Автоматичне масштабування з політиками на основі витрат, контроль використання з ідентифікацією користувачів
CloudHealth by VMware	AWS, Azure, GCP	Частково (через інтеграції та сценарії)	Так	Так	Підтримка відповідності (SOC 2, HIPAA), безпечний доступ через API, журнали аудиту

Кожна з розглянутих платформ має свій функціональний фокус, що визначає її призначення та роль у загальній системі фінансового управління хмарними ресурсами. Зокрема, Apptio Cloudability спеціалізується на глибокому фінансовому аналізі,

прогнозуванні витрат та управлінні довгостроковими фінансовими зобов'язаннями, що робить її особливо ефективною для стратегічного планування бюджету.

Платформа Flexera One поєднує в собі можливості системи CMDB з аналітикою FinOps, забезпечуючи не лише контроль витрат, а й активне управління ресурсами та впровадження політик економії на рівні всієї організації. У свою чергу, Spot by NetApp зосереджена на повній автоматизації процесів оптимізації, з особливим акцентом на середовищах Kubernetes, що робить її привабливим рішенням для команд DevOps у динамічних інфраструктурах, які масштабуються.

Платформа CloudHealth by VMware вирізняється просунутою системою візуалізації витрат та бізнес-орієнтованою аналітикою, адаптованою до потреб користувачів різних рівнів – від технічних спеціалістів до фінансових директорів і топ-менеджменту. Варто зазначити, що всі платформи, за винятком Spot, підтримують прогнозування витрат та надають рекомендації щодо оптимізації. Водночас лише деякі рішення забезпечують глибоку інтеграцію з системами ITSM та CMDB, що є ключовим фактором для побудови повноцінної керованої екосистеми FinOps у мультихмарній архітектурі [24].

Таким чином, вибір платформи має ґрунтуватися на стратегічних цілях організації: чи то контроль і зниження витрат, чи інтеграція з процесами змін, чи створення єдиного джерела істини для прийняття фінансово-технічних рішень.

Інтегровані рішення на базі SIEM/CMDB. Інтегровані рішення на базі систем SIEM або CMDB відіграють особливу роль у побудові системного, процесного та контрольованого підходу до управління витратами у хмарному середовищі. Це не спеціалізовані платформи класу FinOps, проте вони дозволяють:

- Поєднувати фінансову аналітику з поточними IT-процесами.
- Інтегрувати дані про витрати в структуру управління інцидентами, змінами та конфігураціями.
- Запускати автоматизовані сценарії реагування у разі перевитрат або порушення політик.

Найпоширенішими прикладами таких рішень є Splunk (як SIEM/Observability платформа) та Cherwell або ServiceNow (як CMDB/ITSM системи) [25].

Splunk з додатками для хмарного моніторингу та білінгу. Платформа Splunk традиційно використовується як інструмент SIEM для збору, обробки та аналізу логів, подій та операційних метрик у реальному часі. Проте завдяки спеціалізованим додаткам (add-ons) Splunk також може ефективно використовуватися для моніторингу фінансових метрик, зокрема хмарних витрат.

Інтеграція з основними хмарними провайдерами – AWS, Azure та GCP – реалізується через офіційні додатки (наприклад, Splunk Add-on for AWS Billing, Azure Monitor Add-on), які дозволяють автоматично отримувати дані про витрати, бюджети, теги, інстанси та сповіщення про білінг. Зібрана інформація може бути візуалізована в кастомізованих аналітичних дашбордах, де користувачі можуть аналізувати видатки за проєктами, командами чи сервісами, виявляти відхилення від середніх показників та будувати інтегровану мультихмарну звітність [26].

Однією з ключових особливостей Splunk у моніторингу витрат є можливість встановлення індивідуальних порогів для виявлення перевитрат з подальшою автоматичною генерацією сповіщень або сценаріїв ескалації. Для цього використовується система кастомних правил, що дозволяє реагувати через webhook, електронну пошту або інші механізми інтеграції. Крім того, зберігання історичних даних білінгу відкриває можливості для аналізу трендів та довгострокового

прогнозування витрат. Основною перевагою використання Splunk як платформи моніторингу витрат є її високий рівень гнучкості та масштабованості, а також здатність адаптуватися до специфічних потреб корпоративного середовища. Однак використання цього інструменту вимагає базових знань мови запитів Splunk (SPL), налаштування додатків, створення власних дашбордів та логіки реагування, що може потребувати додаткових ресурсів на етапі впровадження [27].

Cherwell та ServiceNow з інтеграцією даних білінгу. Платформи Cherwell та ServiceNow належать до класу рішень ITSM/CMDB і використовуються для моделювання IT-інфраструктури, управління змінами, обробки запитів, інцидентів та пов'язаних сервісних процесів. На додаток до традиційних функцій підтримки IT-операцій, ці системи все частіше застосовуються для інтеграції фінансової інформації, зокрема для моніторингу хмарних витрат та контролю бюджету [28].

Інтеграція з хмарними платформами (AWS, Azure, GCP) реалізується через API або за допомогою посередницьких рішень (MuleSoft, Zapier, кастомні компоненти middleware). Це дозволяє автоматично синхронізувати дані про витрати, бюджети, відповідальних осіб (наприклад, CSA Owner), обсяги щоденного та щомісячного споживання ресурсів, а також відстежувати випадки перевищення встановлених бюджетних лімітів. Ця інформація зберігається в об'єктах бази даних конфігурацій і може бути пов'язана з конкретними проєктами, командами або департаментами.

Ключовою перевагою використання Cherwell або ServiceNow у фінансовому моніторингу є можливість автоматичного створення інцидентів або запитів при досягненні певних порогів витрат. Наприклад, коли використання бюджету хмарного проєкту перевищує 90%, система генерує запит на підтвердження подальшого споживання ресурсів. Якщо відповідь не отримана протягом визначеного періоду (наприклад, 24 годин), створюється інцидент, який спрямовується відповідній команді (FinOps, DevSecOps або менеджеру IT-департаменту). Ці системи також підтримують побудову робочих процесів схвалення (approval workflows) – процесів, що можуть включати запити на збільшення бюджету, доступ до додаткових ресурсів або розгляд нестандартних витрат. Використовуючи правила реагування, користувачі можуть налаштувати, кому і коли надсилати сповіщення, які ескалації ініціювати та які події мають запускатися автоматично. Крім того, платформи пропонують глибоку інтеграцію з інструментами комунікації та розробки, такими як електронна пошта, Microsoft Teams, Slack, Jira або пайплайни DevOps [29].

Перевагою таких CMDB-рішень є їх високий рівень структурованості, управління ролями та зв'язок фінансової інформації з реальними IT-процесами. Вони дозволяють вбудовувати моніторинг витрат безпосередньо в життєвий цикл сервісів та інцидентів, забезпечуючи тісну співпрацю між технічними та фінансовими підрозділами організації. Проте варто зазначити, що ці платформи зазвичай не містять глибокої аналітики витрат «з коробки» і потребують налаштування інтеграцій, кастомізації логіки реагування та розробки власних звітів чи дашбордів. Хоча Splunk, Cherwell та ServiceNow не є класичними FinOps-платформами, вони відіграють важливу роль у забезпеченні інтегрованого підходу до управління витратами у хмарних середовищах. Завдяки своїй функціональності ці системи дозволяють не лише збирати та зберігати дані про витрати, а й вбудовувати моніторинг фінансових подій безпосередньо в операційні IT-процеси.

Такі рішення сприяють розвитку процесного підходу до контролю витрат, де фінансові метрики пов'язані з подіями життєвого циклу сервісів – змінами конфігурації, інцидентами та запитами на обслуговування. Це дає змогу створювати гнучку логіку

реагування, що враховує організаційні ролі, угоди про рівень послуг (SLA) та рівні відповідальності в IT-структурі [30].

Ці інструменти є особливо цінними для організацій, які вже використовують Splunk або CMDB-рішення, оскільки вони дозволяють інтегрувати управління витратами в наявну інфраструктуру сервісів та моніторингу, уникаючи потреби розгортати окрему FinOps-платформу. Такий підхід підвищує ефективність крос-функціональної взаємодії між IT- та фінансовими департаментами, забезпечуючи прозорість, контроль та підзвітність у використанні хмарних ресурсів.

Інтегровані рішення на базі SIEM/CMDB для спостережності за витратами. У сучасних IT-організаціях інтегровані платформи, що поєднують можливості моніторингу, управління подіями, управління конфігураціями та сервіс-менеджменту, дедалі частіше застосовуються для спостережності за витратами в мультихмарних середовищах. До них належать SIEM-системи, такі як Splunk, та CMDB/ITSM-платформи, такі як Cherwell і ServiceNow. Хоча ці рішення не є спеціалізованими інструментами FinOps, їхня здатність вбудовувати фінансові дані в наявні операційні робочі процеси та процеси безпеки забезпечує гнучкий контроль бюджету та операційну відповідність.

Як було показано в Розділі 2.2 (табл. 1), ці інтеграції безпосередньо підтримують TSC SOC 2 шляхом кореляції аномалій витрат із даними про конфігурації та події для виявлення, ескалації та мінімізації фінансових ризиків. Замість повторного пояснення концепцій SOC 2, цей розділ зосереджується на тому, як такі інтеграції транслюють ці критерії у вимірювані технічні результати в межах мультихмарного врядування [31].

Кейси використання, узгоджені з SOC 2. Інтеграція платформ SIEM та CMDB у робочі процеси моніторингу витрат дозволяє реалізувати операційні сценарії, що відповідають конкретним критеріям SOC 2:

- Виявлення аномалій на основі безпеки – кореляція аномалій витрат із логами подій безпеки у Splunk для виявлення несанкціонованого надання ресурсів або зловживання ними (CC6.1, CC7.2).
- Забезпечення відповідності політикам – автоматичне створення інцидентів у ServiceNow або Cherwell при перевищенні бюджетних порогів, пов'язаних із обмеженнями політик (CC7.3, PI1.1).
- Захист доступності – пріоритезація критично важливих робочих навантажень у CMDB для гарантування того, що на них не вплине вичерпання бюджету (A1.2).
- Готовість до аудиту та підзвітність – комбіноване логування у SIEM/CMDB сповіщень про витрати, ескалацій та схвалень на основі ролей (CC7.4, CC6.6).

Ці кейси демонструють, що платформи SIEM та CMDB можуть слугувати невід'ємними компонентами середовища контролю, узгодженого з SOC 2, гарантуючи, що аномалії витрат контролюються з такою ж суворістю, як і інші інциденти безпеки [32].

Покриття ризиків згідно з SOC 2 через інтеграцію SIEM/CMDB. Сценарії ризиків, визначені в розділі 2.2, вирішуються шляхом інтеграції функціональних можливостей SIEM та CMDB у процеси моніторингу витрат. Завдяки кореляції фінансової та операційної телеметрії, ці системи забезпечують превентивні та детективні заходи контролю, які безпосередньо знижують ймовірність та вплив ідентифікованих загроз. Таблиця 3 підсумовує цю відповідність, показуючи кожен критерій SOC 2 із прикладом його реалізації, станом «до/після» та кількісним покращенням [33].

Таблиця 3

Розширене зіставлення покращень контролю SOC 2 через інтеграцію SIEM/CMDB

Критерій SOC 2	Стан до впровадження	Стан після впровадження	Вплив на покращення / охоплення
CC7.3 Реагування на інциденти	Нові ресурси могли розгортатися непоміченими через неефективну систему сповіщень	Сповіщення у Splunk створює інцидент у ServiceNow, якщо новий ресурс з'являється без схваленого запису про зміни у CMDB; ескалація автоматично призначається відповідальній команді DevSecOps.	Зменшує потребу в ручному нагляді приблизно на 50%; прискорює ескалацію несанкціонованих розгортань та покращує відстежуваність інцидентів.
CC6.6 Управління змінами	«Тіньові» навантаження залишаються необліковаными, що призводить до неконтрольованих витрат і порушення відповідності	Звірка даних CMDB із білінговими даними автоматично ідентифікує навантаження, не пов'язані з зареєстрованими активами; неврегульовані розбіжності генерують тікети щодо відповідності.	Забезпечує 100% видимість активів; зменшує розбіжності в конфігураціях (configuration drift) та прогалини у відповідності приблизно на 40%.
A1.2 Доступність	Вичерпання бюджету могло спричинити перебої в роботі критично важливих навантажень	Пріоритезація активів у CMDB запускає сповіщення у Splunk для масштабування (зменшення) некритичних інстансів, якщо прогноз перевищення бюджету > 90%.	Підтримує відповідність вимогам SLA; мінімізує ризик перебоїв у обслуговуванні приблизно на 35%.
CC7.2 Моніторинг	Неправильно налаштовані сповіщення затримують виявлення аномалій	Правила кореляції SIEM позначають випадки, коли канали сповіщень про витрати виходять із ладу або спрацьовують некоректно; автоматична перевірка кожні 6 годин.	Скорочує час реагування приблизно на 45%; підвищує надійність виявлення та охоплення SOC.
CC7.4 Логування аудиту	Зловживання ресурсами могло залишатися непоміченим через відсутність відстежуваності	Комбіновані логи Splunk та CMDB формують повний аудиторський слід аномалій, сповіщень та ескалацій; термін зберігання даних ≥ 1 року.	Дозволяє проводити форензік-розслідування; підтримує готовність до аудиту SOC 2 Типу II з повним ланцюжком доказів.

Це зіставлення, узгоджене з SOC 2, підтверджує, що фінансова спостережність, інтегрована в платформи SIEM та CMDB, виходить за межі врядування витратами та переходить у домен операційної безпеки. Чітко пов’язуючи ризики з критеріями TSC та кількісно оцінюючи покращення, таблиця демонструє, як інтеграція підтримує як превентивні, так і детективні заходи контролю. Кожен сценарій не лише зміцнює відповідність SOC 2, а й підвищує здатність організації виявляти, локалізувати та усувати інциденти, що мають фінансові наслідки та наслідки для безпеки. Такий структурований підхід гарантує, що ризики, пов'язані з витратами, контролюються в тому ж середовищі, що й інші критичні процеси безпеки, тим самим підвищуючи як готовість до аудиту, так і операційну стійкість [34].

Ці рішення є особливо ефективними для організацій, які вже мають налагоджену систему управління сервісами або використовують Splunk як платформу SIEM/Observability. У таких випадках інтеграція фінансового моніторингу в наявні IT-процеси є логічним і економічно вигідним кроком, що забезпечує високу прозорість, підзвітність і контроль над використанням хмарних ресурсів [35].

Опис запропонованого рішення для моніторингу витрат у мультихмарному середовищі. Запропоноване рішення є інтегрованою системою контролю витрат для мультихмарної інфраструктури, що поєднує можливості моніторингу, аналізу, сповіщення та автоматизованого реагування на перевищення бюджету. Архітектура базується на платформі Splunk (для збору, агрегації та аналізу даних білінгу) та Cherwell (як система ITSM/CMDB для зберігання даних про бюджети, відповідальних осіб, управління інцидентами та автоматизації процесів реагування).

Система розроблена для виявлення сценаріїв перевитрат у режимі близькому до реального часу та їх ескалації через багаторівневу логіку сповіщень і відповідальності. Як показано в рівнянні (1), система безперервно оцінює співвідношення фактичних витрат C(t) до затвердженого бюджету B, запускаючи події ескалації T_k кожного разу, коли перевищується поріг θ_k [36].

Рівняння (2) визначає поведінку системи у разі відсутності вчасного реагування з боку відповідальної сторони. Якщо споживання бюджету перевищує 110% і реакція не з'являється протягом часового вікна τ, інцидент ескалується на команду DevSecOps. З рівняння (3) випливає, що якщо абсолютне відхилення δ(t) перевищує заздалегідь визначену маржу перевитрат γ, інцидент передається команді SecOps незалежно від попередньої ескалації чи підтвердження.

Логіка сповіщень формалізована в рівнянні (4) як кусково-задана функція N(t), що забезпечує інформування відповідних зацікавлених сторін – включаючи власника бюджету, менеджера проєкту та CSA – на відповідних етапах ескалації.

Ключовою особливістю рішення є його адаптивність до будь-якого хмарного середовища (AWS, Azure, Google Cloud) та здатність працювати з кількома провайдерами одночасно, забезпечуючи єдину точку аналітики та контролю.

Переваги запропонованого рішення. Архітектура розробленої системи моніторингу витрат має низку переваг, що забезпечують її ефективність у складних мультихмарних середовищах.

По-перше, повна мультихмарність: Рішення забезпечує уніфікований моніторинг та аналітику для різних хмарних провайдерів (AWS, Azure, GCP), дозволяючи уникнути фрагментації даних і створити єдине інформаційне середовище для прийняття рішень.

По-друге, автоматизація процесів: Значний акцент зроблено на автоматизації збору даних, розрахунку порогів, сповіщень, створення інцидентів та ескалації. Це мінімізує ручне втручання, скорочує час реагування та підвищує надійність системи [40].

Третя перевага – структурована модель ескалації: Забезпечує контроль витрат на кожному етапі зростання, враховуючи рівень критичності та зобов'язання залучених учасників.

Четверте, інтеграція з бізнес-ролями: Система враховує не лише технічні параметри, а й організаційні повноваження, дозволяючи фінансовим, операційним та технічним командам спільно брати участь у прийнятті рішень щодо використання хмарних ресурсів.

Нарешті, прогнозування витрат: Завдяки інтеграції зі Splunk реалізовано можливість генерації аналітичних звітів, ідентифікації трендів та оцінки майбутніх потреб у ресурсах, що формує основу для стратегічного планування бюджету.

Математична модель для розрахунку порогів та аналізу відхилень у мультихмарних середовищах. Для ефективного управління витратами на хмару та підтримки своєчасної ескалації інцидентів пропонується наступна математична модель.

Вона забезпечує структурований метод розрахунку бюджетних порогів, виявлення відхилень та ініціювання процесів реагування на основі фінансових аномалій.

Позначення:

- B: Затверджений бюджет для даного проєкту на визначений період часу (наприклад, місяць), виміряний у грошових одиницях.
- C(t): Фактичні витрати на хмару в момент часу t.
- δ(t)=C(t) – B: Абсолютне відхилення від бюджету в момент часу t.
- $\theta_k \in (0,1]$: Бюджетний поріг для рівня ескалації k, де:
  - $\theta_1 = 0.7$: Жовтий рівень – раннє попередження;
  - $\theta_2 = 0.9$: Помаранчевий рівень – підвищений ризик;
  - $\theta_3 = 1.0$: Червоний рівень – повне вичерпання бюджету або перевитрати.
- γ: Поріг абсолютної суми перевищення для запуску критичного інциденту (наприклад, 2000 USD).
- T_k: Подія ескалації, що запускається при досягненні порогу θ_k.
- τ: Максимально допустимий час (у годинах або днях) без відповіді від відповідальної сторони (наприклад, CSA).

Ескалація на основі порогів. Для кожного рівня ескалації k∈{1,2,3} оцінюється наступна умова:

$$\frac{C(t)}{B} \geq \theta_k \tag{1}$$

Якщо ця нерівність справджується, запускається подія T_k, що ініціює відповідний процес сповіщення та реагування.

Ескалація за умови відсутності вчасної відповіді. Якщо система виявляє, що:

$$\frac{C(t)}{B} \geq 1.1 \text{ and } \Delta t \geq \tau \tag{2}$$

де Δt – тривалість періоду без підтвердження або коригувальних дій з боку відповідальної сторони, інцидент ескалується на команду DevSecOps.

Виявлення критичного перевищення. Якщо абсолютне відхилення перевищує заздалегідь визначений критичний поріг:

$$\delta(t) = C(t) - B \geq \gamma \tag{3}$$

інцидент негайно передається команді SecOps, незалежно від статусу попереднього реагування.

Функція сповіщення. Кусково-задана функція сповіщення може бути формалізована як:

$$N(t) = \begin{cases} \text{send\_notice}(T_1, \text{BudgetOwner}), & \text{if } \theta_1 \leq \frac{C(t)}{B} < \theta_2 \\ \text{send\_notice}(T_2, \{\text{BudgetOwner, ProjectManager}\}), & \text{if } \theta_2 \leq \frac{C(t)}{B} < \theta_3 \\ \text{send\_notice}(T_3, \{\text{BudgetOwner, ProjectManager, CSA}\}), & \text{if } \frac{C(t)}{B} \geq \theta_3 \end{cases} \tag{4}$$

Ця функція забезпечує інформування відповідних стейкголдерів залежно від суворості споживання бюджету.

Метрика кумулятивного відхилення. Для моніторингу сукупного впливу витрат протягом часу може використовуватися інтегральна метрика відхилення:

$$D = \int_0^T | C(t) - B | dt \quad (5)$$

Альтернативно, для систем з дискретними часовими інтервалами (наприклад, щоденний білінг), доречною є форма суми:

$$D = \sum_{i=1}^{n} | C_i - B | \quad (6)$$

Це дає уявлення про довгострокові відхилення від запланованого бюджету.

Модель прогнозування. Прогнозування витрат на хмару є необхідним для проактивного управління бюджетом та своєчасного виявлення аномалій. У контексті фінансової спостережності як заходу контролю безпеки, прогностичні моделі дозволяють організаціям заздалегідь передбачати порушення порогів, що дає можливість для ранніх дій з мінімізації ризиків і знижує ймовірність неконтрольованих перевитрат.

Лінійне прогнозування витрат. Припускаючи, що витрати на хмару зростають приблизно лінійно з часом (поширений сценарій для стабільних робочих навантажень), для прогнозування майбутніх витрат можна використовувати просту модель лінійної регресії:

$$\hat{C}(t) = \alpha t + \beta \quad (7)$$

Де:

- C̑(t) – прогнозовані сукупні витрати в момент часу t;
- α – оціночна швидкість зростання витрат за день (або годину);
- β – вільний член, що представляє початкові накопичені витрати (часто дорівнює 0 на початку циклу білінгу);
- t – часова змінна (у днях або годинах з початку періоду білінгу).

Ця модель може бути побудована на основі історичних даних поточного циклу білінгу (наприклад, перші 7-10 днів місяця) за допомогою методу найменших квадратів.

Оцінка часу досягнення порогу. Щоб оцінити, коли буде порушено конкретний поріг витрат θ_k·B, ми розв'язуємо рівняння:

$$\hat{C}(t_k^*) = \theta_k \cdot B \quad (8)$$

Розв'язуючи для t_k^*:

$$t_k^* = \frac{\theta_k \cdot B - \beta}{\alpha} \quad (9)$$

Цей вираз дає оціночний час (у днях або годинах), у який витрати досягнуть порогового рівня θ_k (наприклад, 70%, 90% або 100% виділеного бюджету B).

Точність прогнозу та межа похибки. Для підвищення надійності модель може включати довірчий інтервал, використовуючи стандартний аналіз похибок лінійної регресії. Наприклад, верхня межа прогнозу може бути визначена як:

$$\hat{C}_{\text{upper}}(t) = \hat{C}(t) + z \cdot \sigma \quad (10)$$

Де:

σ – стандартна похибка прогнозу,

z – z-оцінка, що відповідає бажаному рівню довіри (наприклад, 1,96 для 95%).

Порівнюючи як нижню, так і верхню межі з визначеними порогами, система може запускати превентивні попередження ще до того, як відбудеться фактичне порушення.

Можливість розширення на інших постачальників хмарних послуг. Хоча запропонована система оцінювалася на прикладі трьох найбільших публічних хмарних провайдерів (AWS, Azure та GCP), її архітектура розроблена з можливістю розширення на додаткових постачальників хмарних послуг (CSP). Основною вимогою є наявність стандартизованих даних про білінг та використання ресурсів, які можна отримати програмним шляхом та нормалізувати. Зокрема, інтеграція з новими CSP вимагає:

1. Доступні API білінгу – CSP повинен надавати програмний доступ до даних про витрати та споживання у структурованому форматі (наприклад, JSON, CSV або REST-ендпоінти).
2. Гранулярність метаданих ресурсів – дані білінгу мають включати ідентифікатори ресурсів, теги або прив'язку до проєктів, що дозволяє узгоджувати їх з активами в CMDB та політиками розподілу витрат.
3. Можливості стрімінгу подій або експорту – для забезпечення виявлення аномалій у режимі близькому до реального часу, CSP повинен підтримувати запланований експорт або інтеграцію на основі подій у платформи SIEM та ITSM.
4. Прозорість безпеки та відповідності – провайдер повинен надавати готові до аудиту записи про витрати та використання, які можна зіставити з TSC SOC 2, забезпечуючи безперервність покриття відповідності.

За наявності цих передумов рішення може бути розширене на нових провайдерів, таких як Oracle Cloud Infrastructure (OCI), IBM Cloud або спеціалізовані регіональні CSP, за умови, що вони надають програмний доступ до білінгу та гранулярність метаданих, порівнянну з AWS, Azure та GCP.

Альтернативні методи прогнозування для підвищення точності . Базовий підхід до прогнозування, застосований у цьому дослідженні, покладається на лінійну регресію, як детально описано в розділі 4.1.7. Хоча ця модель забезпечує інтерпретованість і обчислювальну простоту, вона припускає постійну швидкість зростання витрат у часі. Таке припущення часто є нереалістичним у мультихмарних середовищах, де поведінка витрат може відображати нелінійні тренди, сезонні патерни або закономірності, що залежать від багатьох операційних факторів. Для усунення цих обмежень було розглянуто два альтернативні методи: регресія випадкового лісу (Random Forest Regression) та ядрова регресія (Kernel Regression). Ці моделі забезпечують гнучкість у фіксації нелінійної динаміки витрат і дедалі частіше впроваджуються для операційного прогнозування в складних інфраструктурах.

Регресія випадкового лісу (Random Forest Regression). Регресія випадкового лісу – це метод ансамблевого навчання, який будує множину дерев рішень і усереднює їхні результати для отримання фінального прогнозу. У контексті прогнозування хмарних витрат вхідні ознаки можуть включати:

- Часовий індекс (день, тиждень, місяць);
- Кількість активних віртуальних машин (VM);
- Розподіл типів ресурсів (On-Demand, Reserved, Spot);
- Метрики активності користувачів;
- Сезонні індикатори (місяць, квартал).

Переваги:

- Фіксує складні нелінійні патерни та взаємодії ознак;
- Стійкий до шуму та викидів;
- Надає міри важливості змінних, дозволяючи ідентифікувати фактори, що найбільше впливають на витрати.

Релевантність SOC 2:

Здатність до багатофакторного аналізу сприяє покращенню виявлення аномалій для CC7.2 (Виявлення та моніторинг) та PI1.1 (Цілісність обробки) шляхом кореляції фінансових аномалій з операційними метриками.

Ядрова регресія (оцінювач Надарая-Ватсона). Ядрова регресія – це непараметричний підхід, який оцінює значення в заданій точці як зважене середнє навколишніх спостережень, де ваги визначаються ядровою функцією K(·):

$$\hat{C}(t) = \frac{\sum_{i=1}^{n} K\left(\frac{t - t_i}{h}\right) \cdot C(t_i)}{\sum_{i=1}^{n} K\left(\frac{t - t_i}{h}\right)} \quad (11)$$

де h – параметр ширини смуги (bandwidth), що контролює гладкість кривої.

Переваги:

- Адаптується до локальних варіацій у даних про витрати.
- Ефективний для наборів даних із сезонністю або вибухоподібними патернами.
- Не потребує припущень щодо функціональної форми.

Релевантність SOC 2:

Підвищена точність прогнозу допомагає запобігти вичерпанню бюджету, що відповідає A1.2 (Зобов’язання щодо доступності) та знижує ризик перебоїв у обслуговуванні.

Порівняння методів прогнозування для підвищення точності. Порівняння базується на загальноприйнятих метриках похибок, що зазвичай використовуються в прогнозній аналітиці:

- Корінь із середньоквадратичної помилки (RMSE): Вимірює квадратний корінь із середнього значення квадратів різниць між спостережуваними та прогнозованими значеннями. Більші помилки караються суворіше, що робить RMSE чутливим до значних відхилень.

$$RMSE = \sqrt{\frac{\sum_{i=1}^{n} (y_i - \hat{y}_i)^2}{n}} \quad (12)$$

- Середня абсолютна помилка (MAE): Представляє середнє значення абсолютних різниць між спостережуваними та прогнозованими значеннями. Вона забезпечує пряму інтерпретацію типової помилки прогнозу.

$$MAE = \frac{\sum_{i=1}^{n} | y_i - \hat{y}_i |}{n} \quad (13)$$

- Коефіцієнт детермінації (R^2): Вказує на частку дисперсії в спостережуваних даних, що пояснюється моделлю. Значення, близьке до 1, свідчить про вищу точність прогнозування.

$$R^2 = 1 - \frac{\sum_{i=1}^{n} (y_i - \hat{y}_i)^2}{\sum_{i=1}^{n} (y_i - \bar{y})^2} \quad (14)$$

Для створення стабільного орієнтиру моделі були застосовані до середньомісячних витрат за всі дванадцять місяців 2024 року.

- Спостережувані витрати (середньомісячні): ≈ 97,560 $
- Лінійний прогноз (середнє): ≈ 118,982 $
- Прогноз випадкового лісу (середнє): ≈ 117,792 $
- Ядровий прогноз (середнє): ≈ 117,197 $

Потім набір середньомісячних даних був використаний для розрахунку метрик похибок за період 2024 року (табл. 3).

Таблиця 4

Приклад порівняння методів прогнозування

Модель	RMSE ↓	MAE ↓	R2 ↑	Примітка
Лінійна регресія	11,532	9,847	0.872	Інтерпретована, але обмежена для нелінійних зсувів
Регресія випадкового лісу	9,885	8,126	0.913	Найкраща точність при багатофакторних залежностях
Ядрова регресія	10,143	8,452	0.901	Стійка до сезонних коливань

(↓ нижче – краще, ↑ вище – краще)

Оцінка демонструє, що вдосконалені моделі прогнозування, такі як випадковий ліс та ядрова регресія, забезпечують вимірюваний приріст точності порівняно з лінійною базованою моделлю, зокрема у фіксації нелінійної поведінки та сезонних коливань витрат. Випадковий ліс досяг найвищої точності, тоді як ядрова регресія виявила стійкість в умовах вибухоподібних робочих навантажень.

Проте лінійна регресія залишається цінним компонентом системи оцінювання. Її простота, прозорість і низькі обчислювальні витрати роблять її надзвичайно придатною як базову модель та як інструмент для швидкого проектування витрат у середовищах з обмеженими історичними даними. Крім того, пряма інтерпретованість її коефіцієнтів полегшує комунікацію з фінансовими стейкголдерами та аудиторами, що відповідає вимогам SOC 2 щодо чіткості та підзвітності.

Таким чином, результати пропонують багаторівневий підхід до прогнозування:

- Лінійна регресія для швидких, інтерпретованих базових оцінок.
- Випадковий ліс або ядрова регресія для підвищення точності та стійкості у складних, динамічних мультихмарних середовищах.

Ця багаторівнева методологія збалансовує інтерпретованість, обчислювальну ефективність та точність прогнозування, посилюючи як фінансову спостережність, так і управління ризиками, узгоджене з SOC 2. Принципи, викладені вище, реалізуються за допомогою архітектурних компонентів, описаних у розділі 4.2.

Опис функціональних компонентів архітектурного рішення. Однією з ключових переваг запропонованої системи є її модульна структура, яка дозволяє інтегрувати джерела даних, аналітичне ядро, центр управління подіями та автоматизовану систему сповіщення в єдину платформу для моніторингу витрат у мультихмарному середовищі.

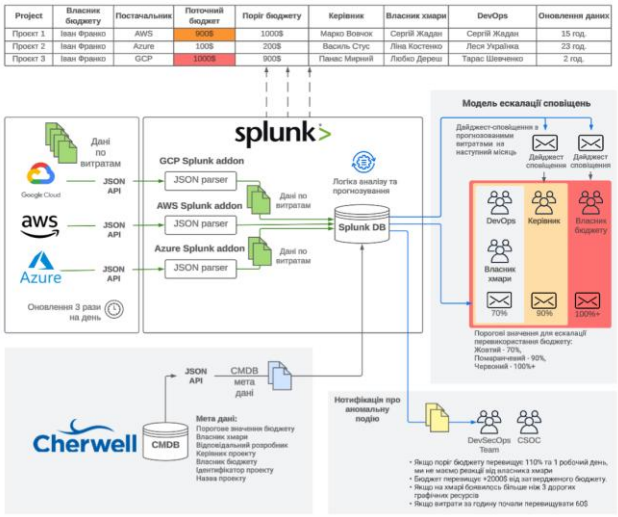

Рис 1. Архітектура рішення з функціональними компонентами

На рівні джерел даних основними постачальниками інформації про хмарні витрати є Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP). Дані про споживання ресурсів та їхню вартість імпортуються через офіційні API у форматі JSON. Частота оновлення встановлена на рівні трьох разів на добу, що дозволяє здійснювати моніторинг фінансових показників у режимі близькому до реального часу [37].

Центральним аналітичним компонентом системи є платформа Splunk, яка виконує функції агрегації та обробки даних про витрати. Для цього використовуються спеціалізовані додатки, зокрема GCP Splunk Add-on, AWS Splunk Add-on та Azure Splunk Add-on, які дозволяють отримувати та обробляти білінгову інформацію з відповідних хмарних платформ. У межах Splunk реалізовано алгоритми для агрегації витрат за провайдерами, проєктами та статтями бюджету, а також для розрахунку частки фактичного споживання в межах встановленого бюджету. Система також підтримує багаторівневу модель ескалації на основі попередньо визначених порогових значень: 70% (умовно «жовтий» рівень), 90% («помаранчевий») та 100% або перевищення бюджету («червоний»).

Рівняння (1)-(4) у сукупності описують логіку, що використовується для визначення тригерів ескалації та сповіщення зацікавлених сторін. Ці обчислювальні моделі створюють прогнозну базу для механізму ескалації, який транслює фінансові аномалії в дієві робочі процеси в межах процесу врядування витратами.

При досягненні кожного порогу можуть створюватися службові замітки та ініціюватися сценарії сповіщення відповідальних сторін.

Ескалація як багатоетапний механізм контролю витрат. Ескалація в цій системі розроблена не лише як технічний тригер, а як структурований багатоетапний механізм врядування. Вона гарантує, що перевитрати обробляються послідовно через визначені рівні відповідальності та автоматизовані робочі процеси.

- Інформаційний рівень (70% бюджету): сповіщення надсилаються власникам бюджетів, що дозволяє їм переглянути тренди споживання.
- Операційний рівень (90%): система автоматично генерує запити на обслуговування в Cherwell або ServiceNow, що вимагає перевірки робочих навантажень або коригування бюджету.
- Критичний рівень (100%+): інциденти високого пріоритету ескалуються на команди DevSecOps та фінансових контролерів із застосуванням захисних заходів, таких як призупинення «тіньових» навантажень або перерозподіл ресурсів.

Ця багаторівнева структура забезпечує ранню обізнаність, операційне втручання та підзвітність керівництва. Шляхом узгодження ескалації з TSC SOC 2 (CC6.1, CC7.2, PI1.1), система не лише запобігає неконтрольованому фінансовому зростанню, а й впроваджує систематичну підзвітність, роблячи фінансові аномалії невід'ємною частиною моніторингу безпеки та відповідності.

Роль у фазах зростання. Ця багаторівнева модель ескалації дозволяє організаціям підтримувати фінансову дисципліну на етапах зростання, коли кількість акаунтів і робочих навантажень швидко збільшується. Ескалація гарантує, що:

- Початкові перевищення розглядаються як ранні попередження, що дозволяє командам реагувати без перебоїв у роботі.
- Повторні або значні відхилення формалізуються в контрольовані процеси, запобігаючи неконтрольованому накопиченню витрат.
- Критичні перевитрати обробляються з видимістю для керівництва та автоматизованими засобами захисту, підтримуючи як бюджетний контроль, так і доступність сервісів.

Завдяки вбудовуванню ескалації в моніторинг витрат, фінансові аномалії не лише виявляються, а й систематично контролюються, що узгоджує контроль витрат із вимогами SOC 2 щодо підзвітності, послідовності та управління інцидентами.

Ескалація та робочий процес автоматизованого реагування. Інформація про бюджетні обмеження, відповідальних осіб та статуси витрат зберігається в системі Cherwell, яка слугує репозиторієм метаданих та центром реагування на події перевитрат. Cherwell фіксує ліміти затверджених бюджетів, ідентифікатори проєктів, дані про відповідальних осіб (CSA) та поточний фінансовий стан кожного об’єкта моніторингу. Коли витрати досягають 90%, система автоматично генерує запит на обслуговування. Якщо фактичне перевищення бюджету становить понад 110% і протягом одного робочого дня не отримано відповіді від відповідального користувача, створюється інцидент, який передається команді DevSecOps для опрацювання. Якщо бюджет перевищено на 2000 доларів понад встановлений ліміт, ініціюється інцидент, що спрямовується до системи інформаційної безпеки (SecOps) [38].

Функціонально важливою частиною архітектури є механізм автоматизованого сповіщення, який забезпечує своєчасну комунікацію з відповідними ролями. Електронні повідомлення надсилаються при досягненні порогів 70%, 90% та 100%. Сповіщення генеруються диференційовано відповідно до рівнів відповідальності: на рівні окремого акаунта – для власника бюджету, а на рівні організації – для CSA або керівника департаменту. Крім того, система генерує щомісячний дайджест, який включає підсумок поточних витрат, аналітику трендів та прогнозні показники на основі моделей, побудованих у Splunk [39].

Для проактивного запобігання перевитратам бюджету система використовує модель лінійного прогнозування витрат, описану в рівнянні (7). Ця модель оцінює очікувані сукупні витрати в даний момент часу на основі поточного темпу зростання

видатків (позначеного коефіцієнтом α) та початкових накопичених витрат на початку періоду білінгу (представлених параметром β).

Далі система розраховує оціночний час t_k^*, у який буде перевищено заздалегідь визначений поріг бюджету (наприклад, 70%, 90% або 100%). Це робиться за допомогою рівняння (9), яке визначає момент часу, коли прогнозовані витрати за планом перетнуть поріг θ_k. Для підвищення надійності та врахування невизначеності система також обчислює верхню межу витрат, включаючи статистичні межі похибки, як визначено в рівнянні (10). Це включає стандартне відхилення прогнозу та довірчий інтервал (виражений через z-оцінку), що дозволяє системі виявляти патерни ризику ще до того, як фактичні витрати досягнуть критичних меж.

Підсумовуючи, ця логіка дозволяє системі не лише виявляти аномалії витрат, а й передбачати їх заздалегідь, покращуючи тим самим планування бюджету та знижуючи ймовірність фінансових інцидентів. Операційна логіка системи базується на принципах максимальної автоматизації для мінімізації ручного втручання. Регулярні оновлення даних, автоматичне створення заміток, інцидентів і запитів, а також вбудовані правила ескалації забезпечують стійкість і передбачуваність системи у реагуванні на зміни фінансових умов.

Для підтримки проактивного управління бюджетом описані механізми доповнюються моделями прогнозування та виявлення аномалій, які додатково підтверджуються шляхом емпіричної оцінки в Розділі 5.

Приклади запитів для впровадження. Для ілюстрації операціоналізації логіки ескалації та моніторингу архітектура може бути доповнена запитами Splunk та SQL, які перетворюють абстрактні пороги на дієві засоби контролю. Ці запити слугують шаблонами для реального розгортання, підтримуючи виявлення аномалій, створення інцидентів та ведення журналів аудиту відповідно до вимог SOC 2.

Запит Splunk для виявлення перевищення порогів бюджету:

```
index=cloud_costs
| eval budget_consumption_ratio = cost_amount / approved_budget
| where budget_consumption_ratio >= 0.7
| eval escalation_level = case(
    budget_consumption_ratio >= 1.0, 3,
    budget_consumption_ratio >= 0.9, 2,
    budget_consumption_ratio >= 0.7, 1
  )
| stats sum(cost_amount) as total_cost by provider_id, escalation_level
```

Цей запит розраховує співвідношення спожитого та затвердженого бюджету, призначає рівень ескалації (1 – інформаційний, 2 – операційний, 3 – критичний) і агрегує витрати за провайдерами. Результат може бути безпосередньо інтегрований із ServiceNow або Cherwell для запуску інцидентів на основі ролей.

SQL-запит для виявлення «тіньових» робочих навантажень:

```
SELECT b.project_id, b.resource_id, b.cost_amount
FROM billing_data b
LEFT JOIN cmdb_assets c
      ON b.resource_id = c.resource_id
WHERE c.resource_id IS NULL
  AND b.billing_date BETWEEN '2024-01-01' AND '2024-01-31'
  AND b.cost_amount > 100;
```

Цей SQL-запит порівнює дані білінгу з активами в CMDB для ідентифікації робочих навантажень, які генерують витрати, але не зареєстровані в офіційній базі даних активів. Такі аномалії представляють потенційне «тіньове IT» (Shadow IT) та неконтрольовані видатки, що можуть бути ескаловані як інциденти щодо відповідності.

На практиці ці запити мають виконуватися за розкладом через регулярні проміжки часу (наприклад, кожні 6 годин для перевірки білінгу, щодня для звірки з CMDB). Хоча часте виконання підвищує операційну видимість, воно також створює експлуатаційні витрати у вигляді викликів API та індексації даних. Організації повинні балансувати між гранулярністю виявлення та ефективністю використання ресурсів.

Приклад практичного сценарію реагування на перевитрати. Для демонстрації операційної логіки запропонованої системи розглянемо типову ситуацію, коли витрати для конкретного проєкту, розміщеного на Google Cloud Platform (GCP), перевищують затверджений бюджет. Припустимо, ліміт використання ресурсів встановлено на рівні 900 доларів, але фактичне споживання досягло 111%, що становить 1000 доларів.

У такому разі система реєструє подію порушення порогу в аналітичному модулі Splunk. Згідно з вбудованою логікою ескалації, це відповідає «червоному рівню» критичності, що вказує на перевитрату бюджету. Splunk негайно ініціює надсилання сповіщення відповідальній особі – власнику CSA.

Якщо протягом 24 годин після сповіщення відповідь не отримана або не вжито коригувальних дій, система автоматично створює інцидент у платформі Cherwell, який потім передається на розгляд команді DevSecOps. Якщо перевитрата продовжує зростати і перевищує затверджений бюджет ще на 2000 доларів, система ініціює створення нового інциденту, цього разу на рівні SecOps, що відповідає за політики безпеки та стратегічне управління ризиками.

Цей сценарій демонструє замкнений цикл автоматизованого контролю витрат, що поєднує технологічні, організаційні та фінансові компоненти процесу реагування. Також варто зазначити, що розроблене рішення не лише забезпечує контроль FinOps, а й сприяє впровадженню певних процедур контролю в рамках підготовки до аудиту SOC 2, включаючи логування дій, дотримання встановлених SLA, реагування на порушення бюджетної політики та збереження історії подій для майбутнього аудиторського огляду.

Результати впровадження системи моніторингу витрат у мультихмарному середовищі. Для оцінки ефективності впровадженого рішення було проведено аналіз динаміки витрат у мультихмарному середовищі за період з квітня 2023 року по березень 2025 року. Оцінка базується на логіці прогнозування та ескалації, формалізованій у рівняннях (1)-(10), де динаміка витрат C(t) аналізується відносно затверджених бюджетів B та визначених порогів θ_1-θ_3. Візуалізація результатів представлена на графіку «Моніторинг витрат для мультихмарної інфраструктури» (рис.2).

Загальний опис графіка. Графік ілюструє зміни трьох основних показників:

- Total Budget (зелена лінія, ліва вісь Y) – загальні витрати на хмарну інфраструктуру.
- Approved Budget (помаранчева лінія, ліва вісь Y) – затверджений бюджет на відповідний період.
- Accounts Number (сіра лінія, права вісь Y) – кількість активних акаунтів, що використовують хмарні ресурси.

На графіку також відображено дві вертикальні кольорові зони, що вказують на ключові етапи впровадження:

- Блакитна зона (2023-04 – 2023-07): період впровадження системи моніторингу витрат.
- Зелена зона (2023-08): початок автоматичних сповіщень кінцевих користувачів у випадках перевитрат.

Динаміка витрат та кількості акаунтів. До впровадження системи (перша половина 2023 року) показник Total Budget залишався відносно стабільним, коливаючись у межах 90 000 - 100 000 доларів. Водночас Approved Budget мав чітко визначений фіксований ліміт (~85 000 - 89 000 доларів). Кількість акаунтів також залишалася стабільною на рівні близько 307.

Після запуску моніторингу в липні 2023 року спостерігається різкий стрибок Total Budget – до 147 056 доларів. Потім, у серпні 2023 року, після запровадження автоматичних сповіщень, витрати зростають ще більше, перевищуючи 185 621 доларів, тоді як Approved Budget зріс лише незначно (~109 839 доларів). Це може свідчити про виявлення накопиченої заборгованості, розкритої системою моніторингу, або про появу раніше прихованих («тіньових») витрат.

Протягом 2023-2024 років Total Budget поступово стабілізується в діапазоні 180 000 -200 000 доларів із незначними коливаннями. Approved Budget демонструє стабільне помірне зростання відповідно до темпів масштабування інфраструктури. Загальна кількість акаунтів також варіюється в межах 304-329, зі зниженням у серпні 2024 року (до 295 акаунтів) та подальшим зростанням до 327 до початку 2025 року.

У першому кварталі 2025 року спостерігається ще один сплеск видатків – Total Budget досягає 247 988 доларів, що може бути пов'язано з масштабуванням системи або підвищенням тарифів хмарних провайдерів. Водночас Approved Budget також зростає до 155 684 доларів, що вказує на адаптацію фінансового планування до змін у структурі споживання.

Ця аномалія, видима як ступінчасте зростання в зеленій зоні на рисунку 2, була ідентифікована як наслідок виявлення тіньових ресурсів та відкладених коригувань білінгу, а не як реальне зростання використання.

Рисунок 2. Динаміка витрат у мультихмарному середовищі з 2023 по 2025 роки. Сплеск у липні-серпні 2023 року відображає виявлення раніше неврахованих ресурсів та звірку білінгу після впровадження системи (див. розділ 5.2)

Оцінка ефективності моніторингу. Впровадження моніторингу витрат та сповіщень користувачів продемонструвало вимірюваний вплив на стабільність бюджету, точність прогнозування та фінансову ефективність (рис. 3).

Два критичні втручання сформували період оцінювання. Ці покращення відповідають моделі прогнозування, описаній у розділі 4.2, яка пов'язує швидкість зростання витрат α та бюджетні пороги θ_1-θ_3 із проактивною генерацією сповіщень:

- Впровадження моніторингу витрат (вересень 2023 року):

Після запровадження моніторингу (блакитна зона) видимість витрат суттєво покращилася. Прогнозні значення (синя лінія) почали тісніше узгоджуватися з фактичним загальним бюджетом (помаранчева лінія), що зменшило розбіжності та дозволило встановити надійну базу для фінансового аналізу.

- Впровадження сповіщень кінцевих користувачів (листопад 2023 року):

Після розгортання системи сповіщень (зелена зона) поведінка користувачів адаптувалася, що призвело до більш стабільних патернів споживання. Це зменшило кількість аномалій, стабілізувало динаміку бюджету та посилило підзвітність на операційному рівні.

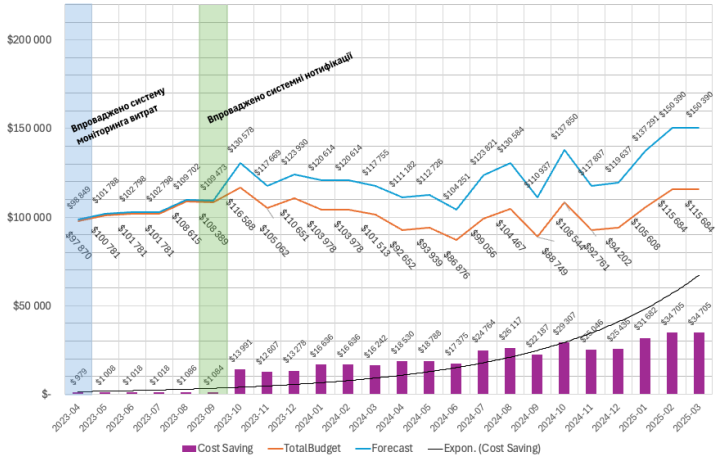

Рисунок 3. Динаміка моніторингу хмарних витрат, прогнозування та економії (2023-2025). Економія розрахована як різниця між базовою траєкторією споживання та фактичними витратами після втручань (методологія детально описана в розділі 5.3.1)

Економія витрат завдяки проактивному моніторингу. Запровадження систематичного моніторингу та сповіщень користувачів призвело не лише до підвищення прозорості, а й до вимірюваних фінансових результатів. На початковому етапі, що припав на середину 2023 року, економія витрат була незначною і не перевищувала 2 000 доларів на місяць. Однак у міру розвитку системи та адаптації поведінки користувачів протягом 2024 року спостерігалося стійке підвищення ефективності, причому щомісячна економія часто перевищувала 15 000-20 000 доларів. До початку 2025 року економія перевищила 34 000 доларів на місяць. Експоненціальна лінія тренду, зображена на Рисунку 3, підкреслює кумулятивний приріст ефективності, зумовлений проактивним моніторингом та коригувальними діями, ініційованими через сповіщення.

Методологія розрахунку економії. Економія витрат, представлена на Рисунку 3, відображає фінансовий вплив проактивного моніторингу та змін у поведінці користувачів після впровадження системи. Економія розраховується як:

$$\text{Savings}(t) = C_{\text{baseline}}(t) - C_{\text{actual}}(t)$$

де C_{baseline} (t) – прогнозована вартість за умови збереження патернів споживання, що були до впровадження, а C_{actual} (t) – фактичні витрати при активному моніторингу.

Базова швидкість α_{baseline} була виведена з даних за квітень-червень 2023 року (середньомісячне зростання 2,3 %):

$$C_{\text{baseline}}(t) = C_0 \times (1.023)^t$$

з $C_{baseline}$=$98,450 (середньомісячна вартість, 2-й квартал 2023 року)

Джерела економії:

1. Ліквідація покинутих ресурсів (42 %) – простоюючі інстанси EC2, неприкріплені томи EBS, зайві знімки (snapshots).
2. Оптимізація розмірів (Right-Sizing) (31 %) – оптимізація інстансів на основі сповіщень рівня 90 %.
3. Оптимізація резервованих інстансів (18 %) – перехід з оплати за запитом (On-Demand).
4. Дострокове припинення тестових середовищ (9 %) – автоматичне вимкнення при досягненні порогу 70 %.

Валідація проводилася з використанням журналів інцидентів Cherwell, звітів про білінг AWS/Azure/GCP та записів фінансової звітності. Сукупна економія (липень 2023 р. – березень 2025 р.) склала $389,400 – зниження на 22,7 % порівняно з базовим прогнозом.

Атрибуція економії. Щоб переконатися, що економія стала результатом системних втручань, а не зовнішніх факторів, таких як коливання ринкових цін або скорочення штату організації, кожне зниження витрат було відстежено до відповідного сповіщення та вирішення інциденту в Cherwell.

Цей аудиторський слід підтвердив, що фінансові покращення виникли внаслідок цілеспрямованих коригувальних дій – таких як видалення покинутих ресурсів, примусове відключення згідно з політиками або впровадження рекомендацій щодо оптимізації розмірів – і все це було ініційовано через автоматичні сповіщення та реакції користувачів.

Таким чином, спостережуване зростання фінансової ефективності можна безпосередньо віднести до впровадженої системи моніторингу та ескалації, а не до зовнішніх економічних умов.

Резюме. Оцінка демонструє, що інтегроване рішення для моніторингу значно підвищило прозорість витрат, зміцнило механізми підзвітності та покращило точність прогнозування. Крім того, система забезпечила стабільну фінансову економію, яка продовжувала масштабуватися з часом. У сукупності ці результати ілюструють перехід організації від реактивної моделі контролю витрат до проактивної системи фінансового врядування, узгоджуючи спостережність за витратами як із цілями відповідності SOC 2, так і з найкращими практиками FinOps.

Обмеження та майбутня робота. Хоча оцінка, заснована на математичній базі, описаній у розділі 4.2, демонструє ефективність, слід визнати кілька обмежень. По-перше, емпіричні результати отримані в результаті розгортання на одному підприємстві, що обмежує можливість узагальнення висновків для різних організаційних контекстів. Хоча для підвищення надійності використовувалися агреговані щомісячні дані за 2024 рік, подальша валідація в різних організаціях та галузях забезпечила б сильнішу зовнішню валідність.

По-друге, аналіз прогнозування був обмежений трьома репрезентативними моделями (лінійна регресія, випадковий ліс та ядрова регресія). Хоча вони охоплюють як інтерпретовану, так і нелінійну поведінку, додаткові методи, такі як градієнтний бустинг, рекурентні нейронні мережі або гібридні ансамблі, можуть забезпечити подальше покращення точності прогнозування.

По-третє, оцінка зосереджувалася на агрегованих витратах на хмару серед усіх провайдерів. Більш детальна розбивка за хмарними сервісами (AWS, Azure, GCP) дозволила б виявляти аномалії та стратегії оптимізації для кожного конкретного провайдера, пропонуючи таким чином глибший погляд на мультихмарні фінансові ризики.

Тому майбутня робота буде зосереджена на розширенні набору даних через численні кейс-стаді, впровадженні додаткових методів прогнозування та проведенні аналізу на рівні провайдерів. Ці розширення не лише покращать наукову строгість оцінки, а й зміцнять практичну застосовність структур спостережності за витратами в хмарних середовищах, узгоджених із SOC 2.

ВИСНОВКИ

У цій статті було розглянуто актуальну проблему моніторингу витрат у мультихмарному середовищі – виклик, з яким стикаються багато сучасних IT-організацій через масштабування інфраструктури, різноманітні моделі білінгу хмарних провайдерів та зростаючі фінансові ризики. Основний акцент було зроблено на необхідності поєднання технічних можливостей із управлінськими практиками для створення послідовного та автоматизованого підходу до відстеження бюджету, прогнозування витрат і своєчасного реагування на інциденти у випадках перевитрат.

Архітектурне рішення, проаналізоване у цій роботі – яке інтегрує можливості Splunk, Cherwell та API білінгу публічних хмар, – демонструє, що така автоматизація дозволяє досягти кількох ключових результатів:

- Централізований та структурований збір даних білінгу з AWS, Azure та GCP.
- Своєчасне виявлення відхилень від бюджету через попередньо визначені пороги.
- Механізми ескалації з чітким розподілом ролей та автоматизованими сповіщеннями.
- Створення інцидентів та запитів на обслуговування у відповідь на порушення бюджету.
- Інтеграція з ширшими бізнес-процесами через інструменти CMDB/ITSM.
- Генерація візуальних прогнозів та стратегічних звітів через Splunk.

Оцінка історичної динаміки витрат показала відчутний вплив після впровадження системи: покращення прозорості фактичних хмарних витрат, стабілізація патернів використання загального бюджету та більш тісне узгодження між затвердженими та спожитими ресурсами. Ці результати відображають покращення фінансової дисципліни та якості прийняття рішень.

Емпіричні результати. Оцінка підтвердила вимірювані переваги. Точність прогнозування покращилася завдяки порівняльному тестуванню моделей (лінійна регресія, випадковий ліс, ядрова регресія), при цьому середньомісячні похибки були кількісно оцінені за допомогою метрик RMSE, MAE та R^2. Фінансова економія стабільно зростала: від незначних значень (менше $2 тис. на місяць у середині 2023

року) до понад $34 тис. на місяць на початку 2025 року, що ілюструє масштабованість проактивного моніторингу.

Порівняно з нативними інструментами CSP (наприклад, AWS Cost Explorer, Azure Cost Management, GCP Billing Reports), запропоноване рішення забезпечило глибшу інтеграцію з процесами ITSM та чітку відповідність критеріям SOC 2, що призвело до вищої прозорості, структурованої ескалації та кращої готовності до аудиту.

Окрім цінності для FinOps, запропоноване рішення також сприяє відповідності та готовності до аудиту, зокрема в контексті стандарту SOC 2. Вбудовуючи ключові засоби контролю, такі як доступ на основі ролей, виявлення аномалій, логування ескалацій та відстежувані робочі процеси, система охоплює кілька критеріїв TSC:

- Цілісність обробки (Processing Integrity). Цей критерій стосується здатності системи забезпечувати повноту, точність і своєчасність обробки даних. У даному випадку це стосується даних про білінг та бюджет із хмарних платформ. Система забезпечує цілісність обробки через автоматизований та запланований збір даних білінгу з AWS, Azure та GCP за допомогою стандартизованих JSON API. Дані оновлюються тричі на день, що гарантує їхню актуальність. Більше того, зібрані дані систематично порівнюються із затвердженими бюджетами, що зберігаються в Cherwell, дозволяючи негайно виявляти невідповідності. Це підтримує узгодженість та надійність даних, що є критично важливим для прийняття фінансових рішень та дотримання нормативних вимог
- Безпека (Security). Критерій безпеки зосереджений на захисті даних від несанкціонованого доступу, модифікації або втрати. У запропонованій моделі безпека підтримується через управління доступом на основі ролей (RBAC), реалізоване як у Splunk, так і в Cherwell. Крім того, система містить вбудовані механізми виявлення аномалій: при перевищенні бюджетних порогів автоматично спрацьовують сповіщення, а у критичних випадках генеруються інциденти.
- Доступність (Availability). У даному випадку забезпечує працездатність та доступність систем навіть при виникненні інцидентів. Рішення вирішує це через проактивні робочі процеси реагування. Своєчасне реагування допомагає запобігти вичерпанню бюджету, що інакше могло б призвести до переривання хмарних послуг або призупинення основних навантажень.
- Моніторингова діяльність (Monitoring Activities). Критерій стосується здатності системи відстежувати та оцінювати ефективність внутрішнього контролю.

Архітектура включає всебічне логування подій, фіксуючи все: від надходження даних білінгу до створення сповіщень та інцидентів. Логи зберігаються у Splunk та Cherwell, створюючи детальний аудиторський слід, який підтримує як внутрішній нагляд, так і зовнішні аудити.

Таким чином, система не лише оптимізує управління витратами, але й створює чіткий аудиторський слід та документацію фінансових рішень, що є необхідним для проходження оцінювання SOC 2 Type II.

Функціональна ціннісна пропозиція. Окрім свого архітектурного внеску та внеску у відповідність вимогам, запропоноване рішення забезпечує чітку цінність для підприємства. Особливо очевидними є три категорії переваг:

- Автоматизація відповідності: Шляхом вбудовування спостережливості за витратами в операційні робочі процеси, система автоматизує збір доказів та логування ескалацій. Це зменшує ручні зусилля, необхідні для підготовки до аудиту SOC 2, потенційно знижуючи витрати на підготовку до аудиту на величину до 70%.

- Зниження ризиків: Безперервний моніторинг фінансових аномалій усуває «сліпі зони», пов’язані з тіньовими робочими навантаженнями та неконтрольованими видатками. Це зміцнює реагування на інциденти та мінімізує вразливість до помилок конфігурації або несанкціонованих розгортань, які несуть як фінансові ризики, так і ризики для безпеки.
- Операційна інтеграція: Фінансові аномалії трансформуються в дієву аналітику безпеки через інтеграцію SIEM/CMDB. Це поєднує FinOps та операції з безпеки, гарантуючи, що фінансові ризики управляються з такою ж суворістю, як і технічні інциденти.

Фінансовий вплив, зафіксований під час оцінювання – із щомісячною економією витрат, що масштабувалася до понад $34 000 до початку 2025 року – може бути безпосередньо пов'язаний зі звітністю підприємства. При проектуванні як повторюваної операційної економії, такі скорочення трансформуються в значні покращення бюджетів департаментів та операційного доходу. Розглянуті як інкрементальні грошові потоки, ці заощадження можуть підтримати фінансування нових проєктів або компенсувати зростання інфраструктури на багаторічних горизонтах, тим самим посилюючи як фінансову дисципліну, так і гнучкість бізнесу.

Це дозволяє IT-організаціям продемонструвати контроль, підзвітність та структуроване реагування на ризики – усе це є критичними факторами в середовищах, де довіра, відповідність та управління даними є важливими для підтримки впевненості клієнтів та партнерів. Таким чином, запропонована архітектура функціонує не просто як інструмент для оптимізації витрат, а як ширша структура врядування та відповідності, яка пов'язує технічні події з фінансовою підзвітністю – підтримуючи як операційну ефективність, так і регуляторну готовність.

Внесок. Ця робота розвиває практичну сторону питання, представляючи моніторинг хмарних витрат як захід контролю безпеки, безпосередньо зіставлений із TSC (Безпека, Доступність, Цілісність Обробки, Моніторингова діяльність) SOC 2. На відміну від існуючих підходів FinOps або CSPM, запропонована система демонструє, як фінансові аномалії можуть розглядатися як сигнали безпеки, поєднуючи операційні фінанси та інформаційну безпеку.

Обмеження та майбутня робота. Поточна оцінка базується на розгортанні на одному підприємстві. Для узагальнення висновків потрібна ширша валідація в організаціях різних розмірів. Крім того, прогнозування було обмежене регресійними та ансамблевими моделями; майбутня робота має включати методи часових рядів (наприклад, ARIMA, Prophet). Успішне впровадження передбачає наявність розвинених практик тегування та інтеграції з CMDB/ITSM, що може бути неможливим у менш зрілих організаціях.

Рекомендації щодо впровадження спостережливості за витратами як заходу контролю безпеки. Щоб впровадити спостережність за витратами як ефективний захід контролю безпеки, організації повинні узгодити свої процеси фінансового моніторингу з існуючими робочими процесами безпеки, відповідності та операцій. Ця інтеграція дозволяє розглядати фінансові аномалії – такі як неочікувані витрати на хмару або відхилення від запланованих бюджетів – не лише як бухгалтерські проблеми, але й як потенційні індикатори неправильної конфігурації, зловживань або системної неефективності. Наступні вказівки окреслюють структурований підхід до впровадження такої моделі.

По-перше, важливо встановити централізований збір даних від усіх хмарних провайдерів, що використовуються. Це передбачає інтеграцію нативних API від таких

платформ, як AWS, Azure та Google Cloud, послідовним автоматизованим способом. Дані про витрати повинні оновлюватися кілька разів на день, щоб забезпечити видимість патернів споживання та дотримання бюджету в режимі близькому до реального часу.

Далі, зібрані дані повинні бути оброблені та проаналізовані за допомогою надійної платформи спостережливості, такої як Splunk. Ця система діє як аналітичне ядро, відповідальне за агрегацію даних, їх порівняння з попередньо визначеними бюджетними порогами та запуск сповіщень. Платформа спостережливості має бути тісно інтегрована з інструментами ITSM, такими як Cherwell або ServiceNow, щоб забезпечити автоматизоване створення запитів на обслуговування або записів про інциденти при порушенні порогів.

Для того, щоб події, пов'язані з витратами, стали дієвими, організації повинні визначити багаторівневу модель ескалації. Наприклад, досягнення 70% визначеного бюджету може запустити попереджувальний електронний лист власнику бюджету проєкту, тоді як перевищення 90% може ініціювати сповіщення ширшим командам, включаючи DevOps та FinOps. Якщо 100% бюджету перевищено і протягом встановленого періоду не вжито жодних коригувальних дій, інцидент має бути ескалований команді безпеки (SecOps або DevSecOps) для подальшого аналізу.

Паралельно, до всіх інтерфейсів моніторингу витрат має бути застосовано суворий контроль доступу на основі ролей (RBAC). Тільки авторизованим особам має бути дозволено отримувати доступ до дашбордів, змінювати пороги або реагувати на події, пов'язані з витратами. Усі дії в системі повинні логуватися, мати позначку часу та зберігатися для підтримки внутрішнього аудиту та зовнішніх перевірок на відповідність.

Можливості прогнозування також є вирішальними. Використовуючи такі інструменти, як Splunk, організації можуть створювати динамічні звіти та прогнози трендів, що дозволяє здійснювати проактивне планування та раннє виявлення потенційних перевитрат. Ці звіти повинні регулярно розповсюджуватися як серед технічних, так і серед фінансових стейкголдерів для полегшення спільного прийняття рішень.

Важливо, що всі ці практики повинні бути зіставлені з TSC SOC 2. Системи спостережливості за витратами сприяють Цілісності обробки, забезпечуючи точність і своєчасність білінгових даних; Безпеці шляхом контролю доступу та виявлення аномалій; Доступності шляхом запобігання перервам у роботі сервісів через неконтрольоване вичерпання бюджету; та Моніторинговій діяльності через всебічне логування подій та візуальну аналітику.

Нарешті, успішне розгортання такої системи залежить від співпраці між командами FinOps, DevOps та безпеки. До сигналів, пов’язаних із витратами, слід ставитися з таким самим рівнем операційної терміновості, як і до інших аномалій інфраструктури, закриваючи розрив між фінансовим наглядом та станом безпеки.

Підсумовуючи, впровадження спостережливості за витратами як заходу контролю безпеки дозволяє організаціям не лише зменшити фінансовий ризик, але й побудувати більш стійку, прозору та готову до аудиту мультихмарну інфраструктуру.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Alexander, K., Hanif, M., Lee, C., Kim, E., & Helal, S. (2020). Cost-aware orchestration of applications over heterogeneous clouds. *PLOS ONE, 15*(2), e0228086. https://doi.org/10.1371/journal.pone.0228086

2. Shokotko, L., Suprun, A., Petrishyna, T., & Pavlysh, T. (2024). Cloud cost monitoring and forecasting: Issues and challenges. *Economics and Technical Engineering*, *2*(2), 58–75. https://doi.org/10.62911/ete.2024.02.02.05
3. Wojtowicz, D. T., Yin, S., Martinez-Gil, J., Morvan, F., & Hameurlain, A. (2022). Multi-cloud query optimisation with accurate and efficient quoting. In *Proceedings of the IEEE International Conference on Big Data*. https://doi.org/10.1109/BigData55660.2022.10020835
4. Li, F., Wu, G., Lu, J., Jin, M., An, H., & Lin, J. (2022). SmartCMP: A cloud cost optimization governance practice of smart cloud management platform. In *Proceedings of IEEE SmartCloud* (pp. 171–176).
5. Thumala, S. R., & Pillai, B. S. (2024). Cloud cost optimization methodologies for cloud migrations. *International Journal of Intelligent Systems and Applications in Engineering*, *12*(2), 4797–4809.
6. Konidena, S. (2024). Cost-effective scalability in cloud monitoring systems: A comparative study. *International Journal of Innovative Science and Research Technology*, 382–385. https://doi.org/10.38124/ijisrt/IJISRT24AUG641
7. Chornii, V., Martseniuk, Y., Partyka, A., & Harasymchuk, O. (2025). Information security risks associated with the uncontrolled storage of secrets in source code. In *CEUR Workshop Proceedings*, *4042* (pp. 250–271).
8. Piskozub, A., & Abibulaiev, A. (2025). Integration of NLP and ML in cloud infrastructure security. In *CEUR Workshop Proceedings*, *4024* (pp. 260–275).
9. Kamal, A., Sabry, M., Ali-Eldin, A., & Mohamed, M. (2024). Low-cost IoT air quality monitoring station using cloud platform and blockchain technology. *Applied Sciences*, *14*, 5774. https://doi.org/10.3390/app14135774
10. Deineka, O., & Bortnik, L. (2024). Methodology for collecting, processing, storing, and classifying data in accordance with SOC 2 Type 2 requirements. *Computer Systems and Networks*, *6*, 36–43. https://doi.org/10.23939/csn2024.01.036
11. Sapsai, O., Martseniuk, Y., Partyka, A., & Harasymchuk, O. (2025). Research on automated security incident management in public cloud environments. In *CEUR Workshop Proceedings*, *4042* (pp. 226–249).
12. Cenaj, E., Maraj, E., & Kuka, S. (2025). Utilizing GIS cloud for monitoring and mosquito control. *Edelweiss Applied Science and Technology*, *9*, 345–352. https://doi.org/10.55214/25768484.v9i3.5211
13. Opirskyy, I., Harasymchuk, O., Partyka, O., Susukailo, V., et al. (2025). Modern methods of ensuring information protection in cybersecurity systems using artificial intelligence and blockchain technology. In O. Harasymchuk (Ed.), *Monograph*. https://doi.org/10.15587/978-617-8360-12-2
14. Banala, S. (2025). Cloud observability: AI-enhanced monitoring for proactive incident management.
15. Mittal, A. (2025). AI-powered DevOps in cloud app modernization: Automating deployments, monitoring, and resilience. https://doi.org/10.13140/RG.2.2.26957.14561
16. Vakhula, O., Opirskyy, I., Vorobets, P., Bobko, O., & Kulinich, O. (2025). Research on policy-as-code for implementation of role-based and attribute-based access control. In *CEUR Workshop Proceedings*, *3991* (pp. 139–157).
17. Vakhula, O., & Opirskyy, I. (2024). Research on security-as-code approach for cloud-native applications based on Kubernetes clusters. In *CEUR Workshop Proceedings*, *3800* (pp. 58–69).
18. Pavlenko, V., Pavlenko, V., Manuylov, V., Kuzhel, V., & Buda, A. (2024). Cloud solutions for data integration and analysis in remote vehicle monitoring. *Journal of Mechanical Engineering and Transport*, 109–117. https://doi.org/10.63341/vjmet/2.2024.109
19. Samad, A., Kieser, J., Chourdakis, I., & Vogt, U. (2024). Developing a cloud-based air quality monitoring platform using low-cost sensors. *Sensors*, *24*. https://doi.org/10.3390/s24030945
20. Deineka, O., Harasymchuk, O., Partyka, A., Obshta, A., & Korshun, N. (2024). Designing data classification and secure storage policy according to SOC 2 Type II. In *CEUR Workshop Proceedings*, *3654* (pp. 398–409).
21. Brid, R. (2025). Monitoring distributed cloud-based microservices applications: Concepts and best practices. *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences*.
22. Harasymchuk, O., Deineka, O., Partyka, A., & Kozachok, V. (2024). Information classification framework according to SOC 2 Type II. In *CEUR Workshop Proceedings*, *3826* (pp. 182–189).
23. Kumar, C. H. (2025). Secure WebCloud: Enforcing security contracts in cloud environments. *International Journal for Research in Applied Science and Engineering Technology*, *13*, 109–115. https://doi.org/10.22214/ijraset.2025.67187

24. Venkatesh, K., Konijeti, J., Inavoli, P., Jujjavarapu, G., & Mandapati, T. (2025). IoT-based air quality monitoring and prediction system. *International Journal for Multidisciplinary Research, 7*. https://doi.org/10.36948/ijfmr.2025.v07i02.40370
25. Pashikanti, S. (2025). Proactive threat detection in cloud ecosystems: SIEM, monitoring, and automated remediation. *International Scientific Journal of Engineering and Management, 4*, 1–7. https://doi.org/10.55041/ISJEM01417
26. Samuel, M., Obira, O., & Sansa, K. (2024). Implementation of infrastructure as code template for low-cost cloud infrastructure operations. *East African Journal of Information Technology*, *7*, 462–474. https://doi.org/10.37284/eajit.7.1.2538
27. Thummala, V., & Singh, P. (2025). Developing cloud migration strategies for cost-efficiency and compliance. *International Journal of Islamic Education Research and Multiculturalism*.
28. Gupta, A., & Singh, S. (2025). Seamlessly integrating SAP Cloud ALM with hybrid cloud architectures for improved operations. *International Journal of Computer Science and Engineering, 13*, 923–954.
29. Yadav, S. (2025). Cloud database optimization: Strategies for performance, scalability, and cost-efficiency. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*, 2958–2967. https://doi.org/10.32628/CSEIT25112738
30. Malaraju, S. (2025). Securing cloud environments with bastion hosts. *International Journal for Multidisciplinary Research, 7*. https://doi.org/10.36948/ijfmr.2025.v07i02.40257
31. Pochu, S., Nersu, S., & Kathram, S. (2024). AI-powered monitoring: Next-generation observability solutions for cloud infrastructure. *Journal of AI-Powered Medical Innovations, 2*, 140–152. https://doi.org/10.60087/Japmi.Vol.02.Issue.01.Id.010
32. Guerbaoui, M., El Faiz, S., Ed-Dahhak, A., Lachhab, A., Benhala, B., Bakziz, Z., Ichou, I., & Selmani, A. (2025). From data to decisions: A smart IoT and cloud approach to environmental monitoring. *E3S Web of Conferences*, *601*. https://doi.org/10.1051/e3sconf/202560100008
33. Patwardhan, A., & Karim, R. (2025). Health monitoring of ground support systems through point-cloud processing: Rockbolts extraction phase. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-025-02758-9
34. Shah, B., Jain, S., & Taqa, A. (2025). Hybrid cloud architectures for multi-modal AI systems.
35. Singh, A. (2025). Intent-based networking in multi-cloud environments. *Journal of Engineering and Applied Sciences Technology*, 1–7. https://doi.org/10.47363/JEAST/2025(7)288
36. Varadaraj, P. (2025). Multi-cloud and hybrid infrastructure: Addressing consistency challenges across cloud providers. *International Journal of Advanced Research in Science, Communication and Technology*, 520–526.
37. Madupati, B. (2025). Kubernetes for multi-cloud and hybrid cloud: Orchestration, scaling, and security challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5076649
38. Perumal, A. P., & Ahire, V. (2025). Multi-cloud observability: Tools and techniques for monitoring and troubleshooting complex hybrid cloud environments. *International Journal on Recent and Innovation Trends in Computing and Communication, 13*.
39. Shelke, P., & Frantti, T. (2025). Exploring the possibilities of Splunk enterprise security in advanced cyber threat detection. In *Proceedings of the International Conference on Cyber Warfare and Security* (pp. 605–613). https://doi.org/10.34190/iccws.20.1.3326
40. Mehta, D. (2021). *Splunk certified study guide: Prepare for the user, power user, and enterprise admin certifications*. https://doi.org/10.1007/978-1-4842-6669-4
41. Smith, J., & Ok, E. (2025). The future of cloud security: How unified security management tools transform multi-cloud policy enforcement.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (32), 2026
ISSN 2663 – 4023

Yevhenii Martseniuk
PhD Student, Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0009-2289-0968
yevhenii.v.martseniuk@lpnu.ua

Oleh Deineka
PhD Student, Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0005-9156-3339
deinekaoleg.86@gmail.com

Oleh Harasymchuk
PhD (Technical Sciences), Associate Professor, Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0000-0002-8742-8872
oleh.i.harasymchuk@lpnu.ua

Taras Lukovskyy
PhD (Technical Sciences), Associate Professor, Department of Information Security
Lviv Polytechnic National University, Lviv, Ukraine
ORCID: 0009-0008-1652-8121
taras.i.lukovskyi@lpnu.ua

INTEGRATION OF FINOPS AND SOC 2 CONTROLS IN THE SECURITY SYSTEM OF MULTI-CLOUD ENVIRONMENTS

Abstract. The problem of ensuring cost transparency and proactive budget control in multi-cloud environments is becoming increasingly relevant for modern IT infrastructures. As organizations scale their use of heterogeneous cloud services, they face challenges related to fragmented billing systems, inconsistent cost metrics, and delays in anomaly detection. In this study, cost observability is considered not merely as a financial function, but as an integral component of an organization's security strategy aligned with the SOC 2 framework. The scientific novelty of this work lies in the integration of cost monitoring tools – specifically Splunk, Cherwell, and cloud APIs based on JSON – with operational and security processes. This enables real-time detection of budget deviations, automated incident escalation, and the implementation of control policies based on financial indicators.

The study presents a forward-looking architecture that introduces a unified cost observability layer across heterogeneous billing systems in multi-cloud environments. The architecture transforms provider-specific formats – including JSON exports from AWS Cost Explorer, Azure Cost Management APIs, and GCP Billing exports to BigQuery – into standardized cost events. These normalized streams form a unified timeline of expenditures relative to standardized budget thresholds, while simultaneously generating consolidated financial telemetry for cross-provider anomaly detection and data correlation.

By rethinking financial data as actionable observability signals, this approach enables a transition from fragmented dashboards to a centralized, audit-ready governance layer that supports compliance, incident response, and financial management. The system also incorporates role-based access control (RBAC), escalation thresholds, and forecasting models, creating a cost management layer of direct relevance to FinOps, DevSecOps, and Compliance teams.

Keywords: multi-cloud infrastructure, SOC 2, cloud security, cost monitoring, budget optimization, FinOps, alert automation, cost forecasting, Splunk, cloud orchestration, cost management, cloud governance.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Alexander, K., Hanif, M., Lee, C., Kim, E., & Helal, S. (2020). Cost-aware orchestration of applications over heterogeneous clouds. *PLOS ONE, 15*(2), e0228086. https://doi.org/10.1371/journal.pone.0228086
2. Shokotko, L., Suprun, A., Petrishyna, T., & Pavlysh, T. (2024). Cloud cost monitoring and forecasting: Issues and challenges. *Economics and Technical Engineering, 2*(2), 58–75. https://doi.org/10.62911/ete.2024.02.02.05
3. Wojtowicz, D. T., Yin, S., Martinez-Gil, J., Morvan, F., & Hameurlain, A. (2022). Multi-cloud query optimisation with accurate and efficient quoting. In *Proceedings of the IEEE International Conference on Big Data*. https://doi.org/10.1109/BigData55660.2022.10020835
4. Li, F., Wu, G., Lu, J., Jin, M., An, H., & Lin, J. (2022). SmartCMP: A cloud cost optimization governance practice of smart cloud management platform. In *Proceedings of IEEE SmartCloud* (pp. 171–176).
5. Thumala, S. R., & Pillai, B. S. (2024). Cloud cost optimization methodologies for cloud migrations. *International Journal of Intelligent Systems and Applications in Engineering, 12*(2), 4797–4809.
6. Konidena, S. (2024). Cost-effective scalability in cloud monitoring systems: A comparative study. *International Journal of Innovative Science and Research Technology*, 382–385. https://doi.org/10.38124/ijisrt/IJISRT24AUG641
7. Chornii, V., Martseniuk, Y., Partyka, A., & Harasymchuk, O. (2025). Information security risks associated with the uncontrolled storage of secrets in source code. In *CEUR Workshop Proceedings, 4042* (pp. 250–271).
8. Piskozub, A., & Abibulaiev, A. (2025). Integration of NLP and ML in cloud infrastructure security. In *CEUR Workshop Proceedings, 4024* (pp. 260–275).
9. Kamal, A., Sabry, M., Ali-Eldin, A., & Mohamed, M. (2024). Low-cost IoT air quality monitoring station using cloud platform and blockchain technology. *Applied Sciences, 14*, 5774. https://doi.org/10.3390/app14135774
10. Deineka, O., & Bortnik, L. (2024). Methodology for collecting, processing, storing, and classifying data in accordance with SOC 2 Type 2 requirements. *Computer Systems and Networks, 6*, 36–43. https://doi.org/10.23939/csn2024.01.036
11. Sapsai, O., Martseniuk, Y., Partyka, A., & Harasymchuk, O. (2025). Research on automated security incident management in public cloud environments. In *CEUR Workshop Proceedings, 4042* (pp. 226–249).
12. Cenaj, E., Maraj, E., & Kuka, S. (2025). Utilizing GIS cloud for monitoring and mosquito control. *Edelweiss Applied Science and Technology, 9*, 345–352. https://doi.org/10.55214/25768484.v9i3.5211
13. Opirskyy, I., Harasymchuk, O., Partyka, O., Susukailo, V., et al. (2025). Modern methods of ensuring information protection in cybersecurity systems using artificial intelligence and blockchain technology. In O. Harasymchuk (Ed.), *Monograph*. https://doi.org/10.15587/978-617-8360-12-2
14. Banala, S. (2025). Cloud observability: AI-enhanced monitoring for proactive incident management.
15. Mittal, A. (2025). AI-powered DevOps in cloud app modernization: Automating deployments, monitoring, and resilience. https://doi.org/10.13140/RG.2.2.26957.14561
16. Vakhula, O., Opirskyy, I., Vorobets, P., Bobko, O., & Kulinich, O. (2025). Research on policy-as-code for implementation of role-based and attribute-based access control. In *CEUR Workshop Proceedings, 3991* (pp. 139–157).
17. Vakhula, O., & Opirskyy, I. (2024). Research on security-as-code approach for cloud-native applications based on Kubernetes clusters. In *CEUR Workshop Proceedings, 3800* (pp. 58–69).
18. Pavlenko, V., Pavlenko, V., Manuylov, V., Kuzhel, V., & Buda, A. (2024). Cloud solutions for data integration and analysis in remote vehicle monitoring. *Journal of Mechanical Engineering and Transport*, 109–117. https://doi.org/10.63341/vjmet/2.2024.109
19. Samad, A., Kieser, J., Chourdakis, I., & Vogt, U. (2024). Developing a cloud-based air quality monitoring platform using low-cost sensors. *Sensors, 24*. https://doi.org/10.3390/s24030945
20. Deineka, O., Harasymchuk, O., Partyka, A., Obshta, A., & Korshun, N. (2024). Designing data classification and secure storage policy according to SOC 2 Type II. In *CEUR Workshop Proceedings, 3654* (pp. 398–409).
21. Brid, R. (2025). Monitoring distributed cloud-based microservices applications: Concepts and best practices. *International Journal of Innovative Research in Engineering & Multidisciplinary Physical Sciences.*

22. Harasymchuk, O., Deineka, O., Partyka, A., & Kozachok, V. (2024). Information classification framework according to SOC 2 Type II. In *CEUR Workshop Proceedings, 3826* (pp. 182–189).
23. Kumar, C. H. (2025). Secure WebCloud: Enforcing security contracts in cloud environments. *International Journal for Research in Applied Science and Engineering Technology, 13*, 109–115. https://doi.org/10.22214/ijraset.2025.67187
24. Venkatesh, K., Konijeti, J., Inavoli, P., Jujjavarapu, G., & Mandapati, T. (2025). IoT-based air quality monitoring and prediction system. *International Journal for Multidisciplinary Research, 7*. https://doi.org/10.36948/ijfmr.2025.v07i02.40370
25. Pashikanti, S. (2025). Proactive threat detection in cloud ecosystems: SIEM, monitoring, and automated remediation. *International Scientific Journal of Engineering and Management, 4*, 1–7. https://doi.org/10.55041/ISJEM01417
26. Samuel, M., Obira, O., & Sansa, K. (2024). Implementation of infrastructure as code template for low-cost cloud infrastructure operations. *East African Journal of Information Technology, 7*, 462–474. https://doi.org/10.37284/eajit.7.1.2538
27. Thummala, V., & Singh, P. (2025). Developing cloud migration strategies for cost-efficiency and compliance. *International Journal of Islamic Education Research and Multiculturalism*.
28. Gupta, A., & Singh, S. (2025). Seamlessly integrating SAP Cloud ALM with hybrid cloud architectures for improved operations. *International Journal of Computer Science and Engineering, 13*, 923–954.
29. Yadav, S. (2025). Cloud database optimization: Strategies for performance, scalability, and cost-efficiency. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 11*, 2958–2967. https://doi.org/10.32628/CSEIT25112738
30. Malaraju, S. (2025). Securing cloud environments with bastion hosts. *International Journal for Multidisciplinary Research, 7*. https://doi.org/10.36948/ijfmr.2025.v07i02.40257
31. Pochu, S., Nersu, S., & Kathram, S. (2024). AI-powered monitoring: Next-generation observability solutions for cloud infrastructure. *Journal of AI-Powered Medical Innovations, 2*, 140–152. https://doi.org/10.60087/Japmi.Vol.02.Issue.01.Id.010
32. Guerbaoui, M., El Faiz, S., Ed-Dahhak, A., Lachhab, A., Benhala, B., Bakziz, Z., Ichou, I., & Selmani, A. (2025). From data to decisions: A smart IoT and cloud approach to environmental monitoring. *E3S Web of Conferences, 601*. https://doi.org/10.1051/e3sconf/202560100008
33. Patwardhan, A., & Karim, R. (2025). Health monitoring of ground support systems through point-cloud processing: Rockbolts extraction phase. *International Journal of System Assurance Engineering and Management*. https://doi.org/10.1007/s13198-025-02758-9
34. Shah, B., Jain, S., & Taqa, A. (2025). Hybrid cloud architectures for multi-modal AI systems.
35. Singh, A. (2025). Intent-based networking in multi-cloud environments. *Journal of Engineering and Applied Sciences Technology*, 1–7. https://doi.org/10.47363/JEAST/2025(7)288
36. Varadaraj, P. (2025). Multi-cloud and hybrid infrastructure: Addressing consistency challenges across cloud providers. *International Journal of Advanced Research in Science, Communication and Technology*, 520–526.
37. Madupati, B. (2025). Kubernetes for multi-cloud and hybrid cloud: Orchestration, scaling, and security challenges. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.5076649
38. Perumal, A. P., & Ahire, V. (2025). Multi-cloud observability: Tools and techniques for monitoring and troubleshooting complex hybrid cloud environments. *International Journal on Recent and Innovation Trends in Computing and Communication, 13*.
39. Shelke, P., & Frantti, T. (2025). Exploring the possibilities of Splunk enterprise security in advanced cyber threat detection. In *Proceedings of the International Conference on Cyber Warfare and Security* (pp. 605–613). https://doi.org/10.34190/iccws.20.1.3326
40. Mehta, D. (2021). *Splunk certified study guide: Prepare for the user, power user, and enterprise admin certifications*. https://doi.org/10.1007/978-1-4842-6669-4
41. Smith, J., & Ok, E. (2025). The future of cloud security: How unified security management tools transform multi-cloud policy enforcement.

Отримано редакцією журналу / Received: 14.01.26
Прорецензовано / Revised: 30.01.26
Схвалено до друку / Accepted: 26.03.26